

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# 

# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 25-May-2018 | 1.0 | Naseer Mohammed | First Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 to refine the safety goals inti high level functional safety requirements. Safety goals, architecture elements, functional safety requirements, validation/verification criteria and methods, warning and degradation concepts are detailed.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | Finally, prove that the system meets these requirements by setting the appropriate verification and validation criteria and methods. |
| Safety\_Goal\_02 | The functional time of the LKA should be reduced |
| Safety\_Goal\_03 | The LDW function shall be turned off when driving on *off road conditions*. |
| Safety\_Goal\_04 | The LKA function shall be deactivated when the camera sensor stopped working and driver should be warned about the deactivation ( car dashboard ) |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images of the environment to detect the position of the car relative to lane lines. |
| Camera Sensor ECU | Analyses images from camera to calculate the car’s relative position with respect to lane |
| Car Display | Responsible for displaying status of (active/inactive) LDW & LKA function on the Car Display. |
| Car Display ECU | Responsible for displaying status of (active/inactive) LDW & LKA function on the Car Display. |
| Driver Steering Torque Sensor | Senses the amount of torque applied to the steering. |
| Electronic Power Steering ECU | Calculates how much torque shall be send to the Motor in order to implement the Lane Assistance functionality |
| 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 | 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 amplitude (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 Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | WRONG | The lane keeping assistance function is activated randomly when camera sensor is not working. |

## 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 | 50ms | LDW vibration torque amplitude less than Max\_Torque\_A mplitude |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | LDW vibration torque amplitude less than Max\_Torque\_Frequency |

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 that the Max\_Torque\_Amplitude chosen is low enough that the driver does not loss control over the car and high enough to be detected by driver. | Validate that the Max\_Torque\_Amplitude chosen is low enough that the driver does not loss control over the car and high enough to be detected by driver. |
| Functional  Safety  Requirement  01-02 | Validate that the Max\_Torque\_Amplitude chosen is low enough that the driver does not loss control over the car and high enough to be detected by driver. | Validate that the Max\_Torque\_Amplitude chosen is low enough that the driver does not loss control over the car and high enough to be detected by driver. |

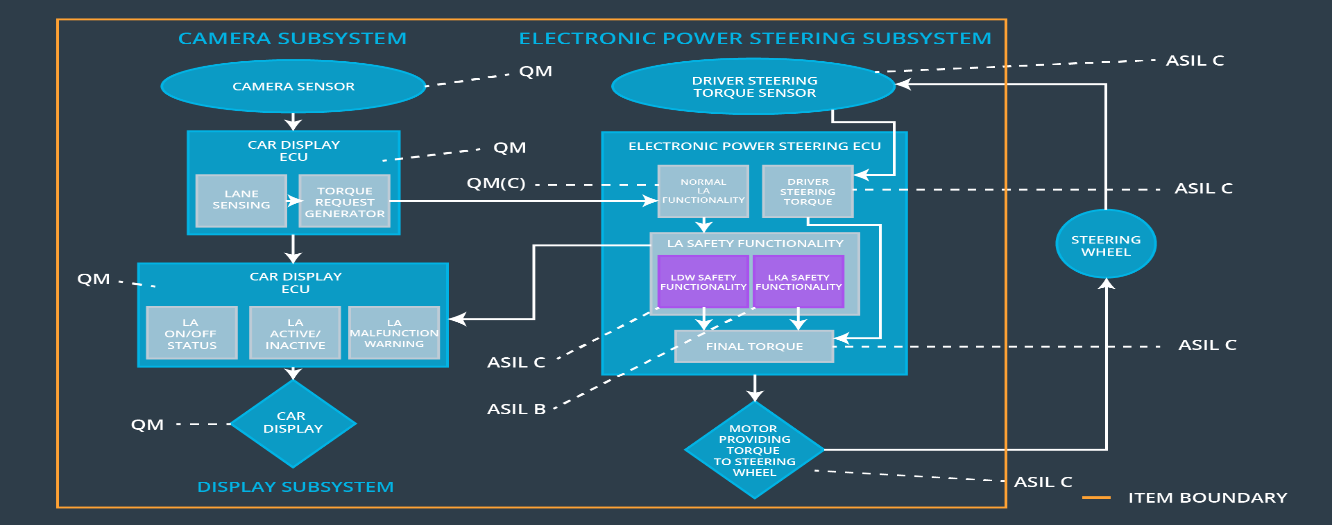
Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | 500ms | Lane Keeping Assistance torque is zero |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall be deactivated​ ​when​ ​the​ ​electronic​ ​power steering​ ​ECU​ ​detects​ ​the​ ​camera sensor​ ​is​ ​not​ ​working. | B | 50ms | Lane Keeping Assistance torque is zero |

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 that the value chosen for Max\_Duration dissuades drivers from taking their hands off the wheel. | Verify that the system does turn off within a fault tolerant time interval, if the lane keeping assistance ever exceeds Max\_Duration |
| Functional  Safety  Requirement  02-02 | Validate​ ​that Lane​ ​Keeping assistance​ ​shall​ ​be​ ​deactivated when​ ​the​ ​camera​ ​sensor​ ​stop working. | Verify that the system does turn off within a fault tolerant time interval, if the camera sensor stopped working. |

## 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 | 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 amplitude is below Max\_Torque\_Amplitude. | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | **X** |  |  |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall be deactivated​ ​when​ ​the​ ​electronic​ ​power steering​ ​ECU​ ​detects​ ​the​ ​camera sensor​ ​is​ ​not​ ​working. | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off LDW functionality | Malfunction\_01,  Malfunction\_02 | Yes | Turn on warning light of the LDW functionality |
| WDC-02 | Turn off LKA functionality | Malfunction\_03,  Malfunction\_04 | Yes | Turn on warning light of the LKA functionality |