

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 7/21/2017 | 1.0 | Deepak Zambre | Initial 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

To associate functional safety requirements with subsystems and elements of a system

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | Oscillating torque from LDW function shall be limited |
| Safety\_Goal\_02 | Lane Keeping Assistance function shall be time limited and additional steering torque shall end after a given time interval, so the driver cannot misuse the system for autonomous driving. |

## Preliminary Architecture

**A close up of a sign

Description generated with high confidence**

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Capture​ ​road​ ​images​ ​and​ ​provide​ ​them​ ​to​ ​the Camera​ ​Sensor​ ​ECU |
| Camera Sensor ECU | Analyze​ ​provided​ ​images​ ​to​ ​calculate​ ​the​ ​car position​ ​on​ ​the​ ​road​ ​respect​ ​to​ ​the​ ​road​ ​lanes |
| Car Display | Provide​ ​feedback​ ​to​ ​the​ ​driver​ ​displaying​ ​warnings and​ ​the​ ​Lane​ ​Departure​ ​Assistance​ ​status |
| Car Display ECU | Manage​​ ​Car​ ​Display​ ​component​ ​to​ ​show​ ​the Lane​ ​Keeping​ ​Assistance​ ​warning​ ​and​ ​Lane Departure​ ​Assistance​ ​status |
| Driver Steering Torque Sensor | Measure​ ​the​ ​torque​ ​applied​ ​to​ ​the​ ​steering​ ​wheel by​ ​the​ ​driver |
| Electronic Power Steering ECU | Use​ ​the​ ​information​ ​received​ ​from​ ​the​ ​Driver Steering​ ​Torque​ ​Sensor​ ​and​ ​the​ ​torque​ ​requested by​ ​the​ ​Lane​ ​Keeping​ ​Assistance​ ​and​ ​Lane Warning​ ​and​ ​request​ ​the​ ​necessary​ ​torque​ ​to​ ​be applied​ ​by​ ​the​ ​Motor​ ​actuator |
| Motor | Applies​ ​the​ ​torque​ ​indicated​ ​by​ ​the​ ​Electronic Power​ ​Steering​ ​ECU​ ​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 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 |

## 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 land departure oscillating torque amplitude is below MAX\_TORQUE\_AMPLITUDE | C | 50ms | Oscillation torque amplitude less than MAX\_TORQUE\_AMPLITUDE |
| 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 | Oscillation torque frequency 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 MAX\_TORQUE\_AMPLITUDE is  - high enough that driver is warned and  - low enough that driver does not loose driving control | Verify: when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval |
| Functional  Safety  Requirement  01-02 | Validate that MAX\_TORQUE\_FREQUENCY is  - high enough that driver is warned and  - low enough that driver does not loose driving control | Verify: when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval |

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 | LKA torque is zero after MAX\_DURATION |

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 chosen MAX\_DURATION really did dissuade drivers from taking their hands off the wheel | Verify: the lane assistance system really does turn off if the lane keeping assistance every exceeded 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 | The lane keeping item shall ensure that the land 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  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only MAX\_DURATION | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | turn off the functionality | Malfunction\_01 Malfunction\_02 | Yes | Warning indicator in dashboard |
| WDC-02 | turn off the functionality | Malfunction\_03 | Yes | Warning indicator in dashboard |