

Functional Safety Concept Lane Assistance

**Document Version: 1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 9/9/2018 | 1.0 | Ajinkya Bhave | Functional Safety Concept for Lane Assistance Item |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_Toc524534664)

[Table of Contents](#_Toc524534665)

[Purpose of the Functional Safety Concept](#_Toc524534666)

[Inputs to the Functional Safety Concept](#_Toc524534667)

[Safety goals from the Hazard Analysis and Risk Assessment](#_Toc524534668)

[Preliminary Architecture](#_Toc524534669)

[Description of architecture elements](#_Toc524534671)

[Functional Safety Concept](#_Toc524534672)

[Functional Safety Analysis](#_Toc524534673)

[Functional Safety Requirements](#_Toc524534674)

[Refinement of the System Architecture](#_Toc524534675)

[Allocation of Functional Safety Requirements to Architecture Elements](#_Toc524534677)

[Warning and Degradation Concept](#_Toc524534678)

# Purpose of the Functional Safety Concept

The Functional Safety Concept derives safety requirements at the functional level from safety goals, allocates each functional safety requirement to the right elements in the functional system architecture, and defines the warning and degradation concepts.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | Oscillating steering torque from LDW function shall be limited |
| Safety\_Goal\_02 | LKA function shall be time limited and additional steering torque shall end after a predefined time interval to prevent driver from misusing the system for autonomous driving |
| Safety\_Goal\_03 | LDW function shall activate within a predefined time interval after receiving a torque request from the camera subsystem |
| Safety\_Goal\_04 | Steering torque from LKA function shall be adequate to keep vehicle in its lane |

## Preliminary Architecture

### 

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images of road in front of the vehicle |
| Camera Sensor ECU | Calculates when the vehicle is leaving the lane  Requests the EPS system to turn and vibrate the steering wheel  Requests the car display system to turn on warning light on dashboard |
| Car Display | Displays warning and status lights for driver |
| Car Display ECU | Turns on warning and status lights on car display |
| Driver Steering Torque Sensor | Detects how much torque the driver is applying to the steering wheel |
| Electronic Power Steering ECU | Processes requests from camera subsystem and driver torque demand and sends final steering torque command to the motor |
| Motor | Applies torque directly to 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 | LDW 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 | LDW function applies an oscillating torque with very high torque frequency (above limit) |
| Malfunction\_03 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | LATE | LDW function applies an oscillating torque after a delay (vehicle has already left the ego lane) |
| Malfunction\_04 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | NO | LKA function is not limited in time duration which leads to misuse as an autonomous driving function |
| Malfunction\_05 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | LESS | LKA function applies a torque that is not adequate in magnitude to keep vehicle centered in lane |

## 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 LA Item shall ensure that the LDW oscillating torque amplitude is below *Max\_Torque\_Amplitude* | C | 50 ms | Turn off LDW |
| Functional  Safety  Requirement  01-02 | The LA Item shall ensure that the LDW oscillating torque frequency is below *Max\_Torque\_Frequency* | C | 50 ms | Turn off LDW |
| Functional  Safety  Requirement  01-03 | The LA Item shall ensure that the LDW oscillating torque is applied within *Max\_ Delay* | C | 50 ms | Turn off LDW |

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 | Normal drivers are able to control the vehicle when torque amplitude is within *Max\_Torque\_Amplitude* | *Criterion*: When the torque amplitude crosses *Max\_Torque\_Amplitude*, the LA output is set to zero within 50 ms  *Method:* Insert torque signal with amplitude greater than *Max\_Torque\_Amplitude* |
| Functional  Safety  Requirement  01-02 | Normal drivers are able to control the vehicle when torque frequency is within *Max\_Torque\_Frequency* | *Criterion:* When the torque frequency crosses *Max\_Torque\_Frequency*, the LA output is set to zero within 50 ms  *Method:* Insert torque signal with frequency greater than *Max\_Torque\_Frequency* |
| Functional  Safety  Requirement  01-03 | Normal drivers are able to steer the vehicle back to lane centre when torque is applied within *Max\_Delay* | *Criterion:* When the torque request is not applied within *Max\_Delay* seconds, the LA output is set to zero within 50 ms  *Method:* Delay the torque signal artificially by more than Max\_Delay seconds |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The EPS ECU shall ensure that the LKA torque is applied for only *Max\_Duration* | B | 500 ms | Turn off LKA |
| Functional  Safety  Requirement  02-02 | The EPS ECU shall ensure that the LKA torque amplitude is greater than *Min\_Torque\_Amplitude* | QM | 500 ms | Turn off LKA |

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 | The *Max\_Duration* value chosen forces drivers not to take their hands off the steering wheel during driving | *Criterion:* When the LKA torque is applied for more than *Max\_Duration* seconds, the LKA output is set to zero within 500 ms  *Method:* Artificially inject torque request from LKA system after *Max\_Duration* seconds |
| Functional  Safety  Requirement  02-02 | The *Min\_Torque\_Amplitude* value chosen is adequate to physically steer the vehicle back to lane centre each time there is deviation | *Criterion:* When the LKA torque applied is less than *Min\_Torque\_Amplitude*, the LKA output is set to zero within 500 ms  *Method:* Artifically reduce LKA torque amplitude below *Min\_Torque\_Amplitude* |

## 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 LA Item shall ensure that the LDW oscillating torque amplitude is below *Max\_Torque\_Amplitude* | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The LA Item shall ensure that the LDW oscillating torque frequency is below *Max\_Torque\_Frequency* | **X** |  |  |
| Functional  Safety  Requirement  01-03 | The LA Item shall ensure that the LDW oscillating torque is applied within *Max\_ Delay* | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The EPS ECU shall ensure that the LKA torque is applied for only *Max\_Duration* | **X** |  |  |
| Functional  Safety  Requirement  02-02 | The EPS ECU shall ensure that the LKA torque amplitude is greater than *Min\_Torque\_Amplitude* | **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, Malfunction\_03 | YES | Warning light on car display |
| WDC-02 | Turn off LKA functionality | Malfunction\_04, Malfunction\_05 | YES | Warning light on car display |