

Functional Safety Concept Lane Assistance

**Document Version:1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 26/11/2018 | 1.0 | Atul Kumar | Draft version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 concept is to identify new system level requirements and

allocate these requirements to high level system diagrams for the lane assistance functional

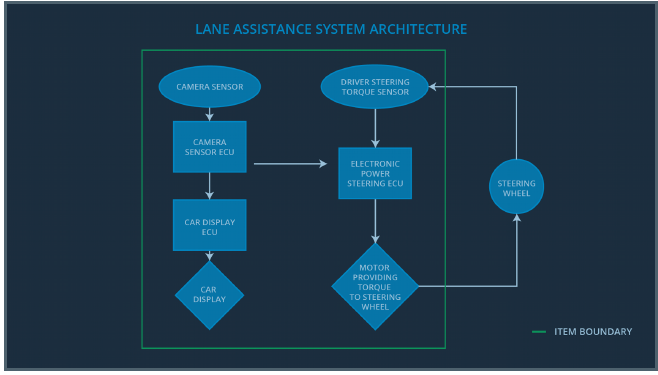
safety project as pertain to the potential malfunctions of the electrical and electronic systems as

defined by ISO 26262 standard or tailored version as per organization.

# 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 (LDW)  function shall be limited |
| Safety\_Goal\_02 | The lane keeping assistance (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 for autonomous driving |
| Safety\_Goal\_03 | The camera sensor ECU shall check the LA on/off, active/inactive and  malfunction warning status before sending torque requests to the lane  departure warning system. |
| Safety\_Goal\_04 | The lane keeping assistance (LKA) function shall deactivate when the  camera sensor stops detecting road markings and shall warn the driver of its deactivation. |



## Preliminary Architecture

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensor responsible for capturing vehicle driving  condition including detectable lane lines. |
| Camera Sensor ECU | Electronic Control Unit (ECU) responsible for detecting  lane lines and determining when the vehicle leaves the  lane by mistake. |
| Car Display | Visual display responsible to displaying warning of lane departures and LKA and LDW activation and  deactivations. |
| Car Display ECU | Electronic Control Unit (ECU) responsible for  displaying warning of lane departures and LKA and  LDW activation and deactivations on the Car Display. |
| Driver Steering Torque Sensor | Sensor responsible for measuring how much force  (steering torque) the driver is applying to the steering  wheel. |
| Electronic Power Steering ECU | Electronic Control Unit (ECU) responsible for  measuring the torque provided by the driver and  adding appropriate amount of torque based on a lane  assistance system torque request (LKA), and vibrates  the steering wheel when the driver drifts away from  center by mistake (LDW). |
| Motor | Actuator responsible for applying requested torque to  the steering column by the Electronic Power Steering  ECU for either the LKA or the LDW functions. |

# 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:  DV04 - Actor effect  (torque amplitude) is  too much. | 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:  DV04 - Actor effect  (torque frequency) is  too much | 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:  DV03 - Function  always activated (No  limit) | 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  lane departure oscillating torque amplitude  is below MAX\_Torque\_Amplitude. | c | 50ms | Set vibration  torque amplitude  to zero. |
| 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 | Set vibration  torque frequency  to zero. |

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  chosen is high enough to be detected by  driver while low enough not to cause  loss of steering. | Verify that the system really does turn  off if the lane departure warning ever  exceeded MAX\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | Validate MAX\_Torque\_Fequency  chosen is high enough to be detected by  driver while low enough not to cause  loss of steering. | Verify that the system really does turn  off if the lane departure warning ever  exceeded MAX\_Torque\_Fequency. |

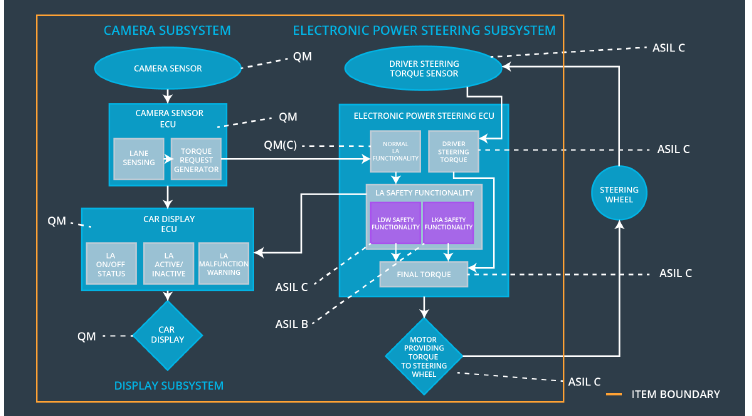
Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 | Set lane keeping assistance torque to 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 Max\_Duration chosen  really did dissuade drivers from taking  their hands off the wheel | Verify that the system really does turn  off if the lane keeping assistance ever  exceeded Max\_Duration |

## Refinement of the System Architecture



|  |  |
| --- | --- |
| Element | Description |
| Camera Sensor | Sensor responsible for capturing vehicle driving  condition including detectable lane lines. |
| Camera Sensor ECU - Lane  Sensing | Software Module in the Camera Sensor ECU  responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. |
| Camera Sensor ECU - Torque  request generator | Software Module in the Camera Sensor ECU  responsible for calculating and sending the additional torque for the LDW and LKA functions. |
| Car Display | Visual display responsible to displaying warning of lane departures and LKA and LDW activation and  Deactivations. |
| Car Display ECU - Lane Assistance  On/Off Status | Visual display responsible to displaying LKA and LDW ON/OFF status. |
| Car Display ECU - Lane Assistant | Visual display responsible to displaying display. |
| Active/Inactive | warning of lane departures, LKA and LDW activation and deactivations. |
| Car Display ECU - Lane Assistance  malfunction warning | Visual display responsible to displaying warning of LKA and LDW malfunctions. |
| Driver Steering Torque Sensor | Sensor responsible for measuring how much force (steering torque) the driver is applying to the steering wheel. |
| Electronic Power Steering (EPS)  ECU - Driver Steering Torque | Software Module in the electronic power steering ECU responsible for receiving the Camera Sensor ECU torque requests. |
| EPS ECU - Normal Lane Assistance  Functionality | Software Module in the electronic power steering ECU responsible for receiving the Driver Steering torque sensor input from the steering wheel. |
| EPS ECU - Lane Departure Warning  Safety Functionality | Software Module in the electronic power steering ECU responsible for keeping the lane departure oscillating torque amplitude and frequence below MAX\_Torque\_Amplitude and MAX\_Torque\_Fequency respectively. |
| EPS ECU - Lane Keeping Assistant  Safety Functionality | Software Module in the electronic power steering ECU responsible for ensuring the application of the lane keeping assistance torque does not ever exceeded Max\_Duration and if lane detection is lost, the LKA function is deactivated. |
| EPS ECU - Final Torque | Software Module in the electronic power steering ECU responsible for ensuring the LDW, LKA and the driver’s steering torque requests are combined and sent to the Motor. |
| Motor | Actuator responsible for applying requested torque to the steering column by the Electronic Power Steering ECU for either the LKA or the LDW functions. |

## 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 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 LDW  functionality | Malfunction\_01,  Malfunction\_02 | Yes, LDW torque  shall be set to  zero | Lane Assist  Inactive and  Malfunction  Warning will be  set in the Car  Display ECU |
| WDC-02 | Turn off LKA  functionality | Malfunction\_03,  Malfunction\_04 | Yes, LKA torque shall be set to zero | Lane Assist  Inactive and  Malfunction  Warning will be  set in the Car  Display ECU |