

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 26/08/2017 | 1.0 | Bide Huang | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

**[Instructions: We have provided a table of contents. If you change the document structure, please update the table of contents accordingly. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In** [**Google Docs**](https://support.google.com/docs/answer/116338?co=GENIE.Platform%3DDesktop&hl=en)**, you can use headings for each section and then go to Insert > Table of Contents.** [**Microsoft Word**](https://support.microsoft.com/en-us/help/285059/how-to-create-a-table-of-contents-by-marking-text-in-word) **has similar capabilities]**

[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 andallocate these requirements to high level system diagrams for the lane assistance functionalsafety project as pertain to the potential malfunctions of the electrical and electronic systems asdefined by ISO 26262 standard.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

**[Instructions:**

**REQUIRED:**

**Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.**

**OPTIONAL:**

**If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.**

**]**

|  |  |
| --- | --- |
| **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. |

## Preliminary Architecture

### 

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Responsible for capturing vehicle driving  condition including detectable lane lines. |
| Camera Sensor 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 | Responsible for communication with Camera ECU and controlling the display device. |
| Driver Steering Torque Sensor | Responsible for measuring how much steering torque the driver is applying to the steering wheel. |
| Electronic Power Steering ECU | Responsible for process driver torque sensor data and add 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 | Actuatating torque request from 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 | 50 ms | 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 | 50 ms | 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  Verify that the system really does turn  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 | 500 ms | 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



## Allocation of Functional Safety Requirements to Architecture Elements

# 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 | Warning of malfunction adn lane assist inactive shall be indicated on Car display. |
| WDC-02 | Turn off LKA  functionality | Malfunction\_03  Malfunction\_05 | Yes, LKA torque  shall be set to  zero | Warning of malfunction adn lane assist inactive shall be indicated on Car display. |