

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 |
| 9/7/2018 | 1.0 | Terry Lu | First Submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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

**[Instructions: Answer what is the purpose of a functional safety concept?]**

Functional safety concept is documents about refining the safety goals into high level functional safety requirements.

# 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 function shall be limited |
| Safety\_Goal\_02 | The lane keeping assistance 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

**[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]**



### Description of architecture elements

**[Instructions: Provide a description for each of the item elements; what is each element's purpose in the lane assistance item? ]**

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Get image data of the road. |
| Camera Sensor ECU | Detect lane from camera image. Identify when the vehicle has accidentally departed its lane. |
| Car Display | Notifications on driver dashboard. |
| Car Display ECU | Sends messages to be displayed by the Car Display. |
| Driver Steering Torque Sensor | records current steering wheel torque. |
| Electronic Power Steering ECU | Decide final steering torque. |
| Motor | Providing torque 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

**[Instructions: Fill in the functional safety analysis table below.]**

|  |  |  |  |
| --- | --- | --- | --- |
| **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 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 | 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

**[Instructions: Fill in the functional safety requirements for the lane departure warning ]**

Lane Departure Warning (LDW) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | The line keeping item shall ensure that the  lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50ms | LDW will set the  oscillating torque  amplitude to 0. |
| Functional  Safety  Requirement  01-02 | The line keeping item shall ensure that the  lane departure oscillating torque frequency is below Max\_Torque\_frequency. | C | 50ms | LDW will set the  oscillating torque  amplitude to 0. |

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 | Criteria: Test how drivers react to different torque amplitudes to prove selection of an appropriate Max\_Torque\_Amplitude  Method: Live driving simulations | Criteria: When torque amplitude  crosses Max\_Torque\_Amplitude, lane  assistance output is set to 0 within 50ms fault tolerant time interval  Method: software test inserting fault into system to observe results |
| Functional  Safety  Requirement  01-02 | Criteria: Test how drivers react to  different torque frequencies to  prove selection of an appropriate Max\_Torque\_Frequency  Method: Live driving simulations | Criteria: When torque frequency  crosses Max\_Torque\_Frequency, lane  assistance output is set to 0 within 50ms fault tolerant time interval  Method: Software test |

**[Instructions: Fill in the functional safety requirements for the lane keeping assistance]**

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 will set  oscillating torque  amplitude to 0. |

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 | Criteria: Test if drivers are dissuaded  from taking hands off wheel based on  selected Max\_Duration value  Method: Live driving simulations | Criteria: When max duration crosses  Max\_Duration, lane assistance output  is set to 0 within 500 ms fault tolerant  time interval  Method: Software test |

## Refinement of the System Architecture

**[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the functional safety lesson including all of the ASIL labels.]**

## Allocation of Functional Safety Requirements to Architecture Elements

**[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Electronic Power Steering ECU** | **Camera ECU** | **Car Display ECU** |
| Functional  Safety  Requirement  01-01 | The line keeping item shall  ensure that the lane departure  oscillating torque amplitude is  below Max\_Torque\_Amplitude. | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The line keeping item shall  ensure that the lane departure  oscillating torque frequency is  below Max\_Torque\_frequency. | **X** |  |  |
| Functional  Safety  Requirement  02-01 | lane keeping assistance function  shall be time limited and the  additional steering torque shall  end after a given timer interval so  that the driver cannot misuse the  system for autonomous driving | **X** |  |  |

## Warning and Degradation Concept

**[Instructions: Fill in the warning and degradation concept.]**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | LDW disabled;  torque request  will be set to 0. | The LDW warning is giving  MORE torque  than what is  safe. | Yes | Warning light  appears on  dashboard. |
| WDC-02 | LKA disabled;  torque request  will be set to 0. | The LKA function had run above  time limit. | Yes | Warning light  appears on  dashboard. |