

Functional Safety Concept Lane Assistance

**Document Version: [Version]**1.0

**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 |
| 06/05/2018 | 1.0 | Efraim Kropp | Initial version |
| 06/19/2018 | 2.0 | Efraim Kropp | Resubmission: Corrected Safe State in section 3.2 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 2](#_Toc517021673)

[Table of Contents 3](#_Toc517021674)

[1. Purpose of the Functional Safety Concept 4](#_Toc517021675)

[2. Inputs to the Functional Safety Concept 4](#_Toc517021676)

[2.1. Safety goals from the Hazard Analysis and Risk Assessment 4](#_Toc517021677)

[2.2. Preliminary Architecture 5](#_Toc517021678)

[2.2.1. Description of architecture elements 5](#_Toc517021679)

[3. Functional Safety Concept 6](#_Toc517021680)

[3.1. Functional Safety Analysis 6](#_Toc517021681)

[3.2. Functional Safety Requirements 7](#_Toc517021682)

[3.3. Refinement of the System Architecture 9](#_Toc517021683)

[3.4. Allocation of Functional Safety Requirements to Architecture Elements 9](#_Toc517021684)

[3.5. Warning and Degradation Concept 10](#_Toc517021685)

# Purpose of the Functional Safety Concept

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

The purpose of the Functional Safety Concept is to refine the safety goals in functional safety requirements and to defining which part of the system architecture will implement each requirement. This could involve expanding the system architecture with new element blocks.

# 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 additional steering torque shall end after given time interval so that the driver could not misuse the system for autonomous driving |
| Safety\_Goal\_03 | The oscillating steering torque from the LDW function shall be high enough for the driver to respond |
| Safety\_Goal\_04 | The Lane Assistance system shall be deactivated when driving on Road with construction site |

## 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 | The Camera Sensor provides road images to the Camera Sensor ECU |
| Camera Sensor ECU | The Camera Sensor ECU detects the lane lines, identifies when the vehicle accidentally departures its lanes and sends appropriate messages to the Car Display ECU and the Electronic Power Steering ECU |
| Car Display | The Car Display displays the warning light on the dashboard |
| Car Display ECU | The Car Display ECU sends a warning light activation signal to the Car Display |
| Driver Steering Torque Sensor | The Driver Steering Torque Sensor measures the torque provided by the driver |
| Electronic Power Steering ECU | The Electronic Power Steering ECU calculates an additional amount of torque for the motor and provides appropriate control signals to the Motor |
| Motor | The Motor provides the torque 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

**[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 LDW 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 LKA 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 Lane Keeping item shall ensure that Lane Departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | The Lane Departure oscillating torque amplitude is set to 0 |
| Functional  Safety  Requirement  01-02 | The Lane Keeping item shall ensure that Lane Departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50ms | The Lane Departure oscillating torque frequency is set 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:  The oscillating torque amplitude never exceeds value Max\_Torque\_Amplitude.  Method:  Set Max\_Torque\_Amplitude to different values and simulate Lane Departure scenario. Measure the output torque amplitude and compare with the Max\_Torque\_Amplitude value. | Criteria:  When the oscillating torque amplitude higher than Max\_Torque\_Amplitude, the output of the system is set to 0 in 50 ms. Observe on the Car Display:   1. The Lane Assist Malfunction Warning light is ON 2. The Lane Assist On/Off status is OFF 3. The Lane Assist Active/Inactive status in INACTIVE   Method:  Apply oscillating torque amplitude higher than Max\_Torque\_Amplitude value |
| Functional  Safety  Requirement  01-02 | Criteria:  The oscillating torque frequency never exceeds Max\_Torque\_Frequency value.  Method:  Set Max\_Torque\_Frequency to different values and simulate Lane Departure scenario. Measure the output torque frequency and compare with the Max\_Torque\_Frequency value. | Criteria:  When the oscillating torque frequency is higher than Max\_Torque\_Frequency value, the output of the system is set to 0 in 50 ms. Observe on the Car Display:   1. The Lane Assist Malfunction Warning light is ON 2. The Lane Assist On/Off status is OFF 3. The Lane Assist Active/Inactive status in INACTIVE   Method:  Apply oscillating torque frequency higher than Max\_Torque\_Frequency value |

**[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 Lane Assistance item shall ensure that the Lane Keeping Assistance torque is applied for only Max\_Duration time | B | 500ms | The Lane Keep Assistance torque output is set 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:  The LKA torque never applied longer than Max\_Duration time.  Method:  Set Max\_Duration to different values and simulate LKA scenario. Measure the duration of the LKA torque and compare with the Max\_Duration value. | Criteria:  When the LKA torque is applied longer than for Max\_Duration time, the output of the system is set to 0 in 500 ms. Observe on the Car Display:   1. The Lane Assist Malfunction Warning light is ON 2. The Lane Assist On/Off status is OFF 3. The Lane Assist Active/Inactive status in INACTIVE   Method:  Apply LKA torque for duration > Max\_Duration |

## 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.]**



We are assuming that a failure of the LKA function does not impact LDW function and keep LKA function software block at ASIL B level.

## 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 Electronic Power Steering ECU shall ensure that Lane Departure oscillating torque amplitude is below Max\_Torque\_Amplitude | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The Electronic Power Steering ECU shall ensure that Lane Departure oscillating torque amplitude 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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | The LDW function is turned off | (1) The Lane Departure oscillating torque amplitude value is MORE than Max\_Torque\_Amplitude  OR  (2) The Lane Departure oscillating torque frequency value is MORE than Max\_Torque\_Frequency | Yes | The Lane Assist Malfunction Warning light is activated on the Car Display |
| WDC-02 | LKA function is turned off | Duration of the applied LKA torque is MORE than Max\_Duration | Yes | The Lane Assist Malfunction Warning light is activated on the Car Display |