

Functional Safety Concept Lane Assistance

**Document Version: [V1.1]**



# 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 |
| 24.01.2019 | V1.1 | Liping S | First version with all required content |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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?]**

The functional safety concept looks at the general functionality of the item. The functional safety concept identify new requirements and allocate these requirements to system diagrams. Allocation means defining which part of the system architecture will implement each requirement.

# 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 steering torque related to lane departure warning shall be limited |
| Safety\_Goal\_02 | LKA function shall only work for a certain amount of time. |
| Safety\_Goal\_03 | LKA shall deactive and inform the driver when the lane detection is failed. |
| Safety\_Goal\_04 | LKA shall provide certainty score of its measurement, and build mechanism to deal with low score situations. |

## 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 | Provide visual signal to camera sensor ECU |
| Camera Sensor ECU | Detect lane line and send behavior target to steering module |
| Car Display | Provide user interface to the driver and show the info of the system |
| Car Display ECU | Convert signal from camera sensor and steering module to visual signal for display |
| Driver Steering Torque Sensor | Sense the steering torque, and send to steering ECU |
| Electronic Power Steering ECU | Process torque sensor signal and send control signal to motor |
| Motor | Receive control signal from steering ECU and apply it 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 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 | The lane departure warning function applies an oscillating  torque with very high 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 | Camera module cannot detect the lane line due to snow |

## 

## 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 the  lane departure oscillating torque amplitude  is below Max\_Torque\_Amplitude | C | 50ms | Function is deactivated |
| 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 | Function is deactivated |

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 | Test and analyze the react of driver to different torque amplitude and find the optimal value | Verify if the system can turn off as expected when exceeding the max torque amplitude |
| Functional  Safety  Requirement  01-02 | Test and analyze the react of driver to different torque frequency and find the optimal value | Verify if the system can turn off as expected when exceeding the max torque frequency |

**[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 steering ECU shall ensure that the  wheel steering torque only be applied in  the Max\_Duration | B | 500ms | LKA torque turns zero |
| Functional  Safety  Requirement  02-02 | The LKA shall be deactivated when the Camera ECU outputs that the lane detection is failed | A | 50 ms | Function is deactivated |

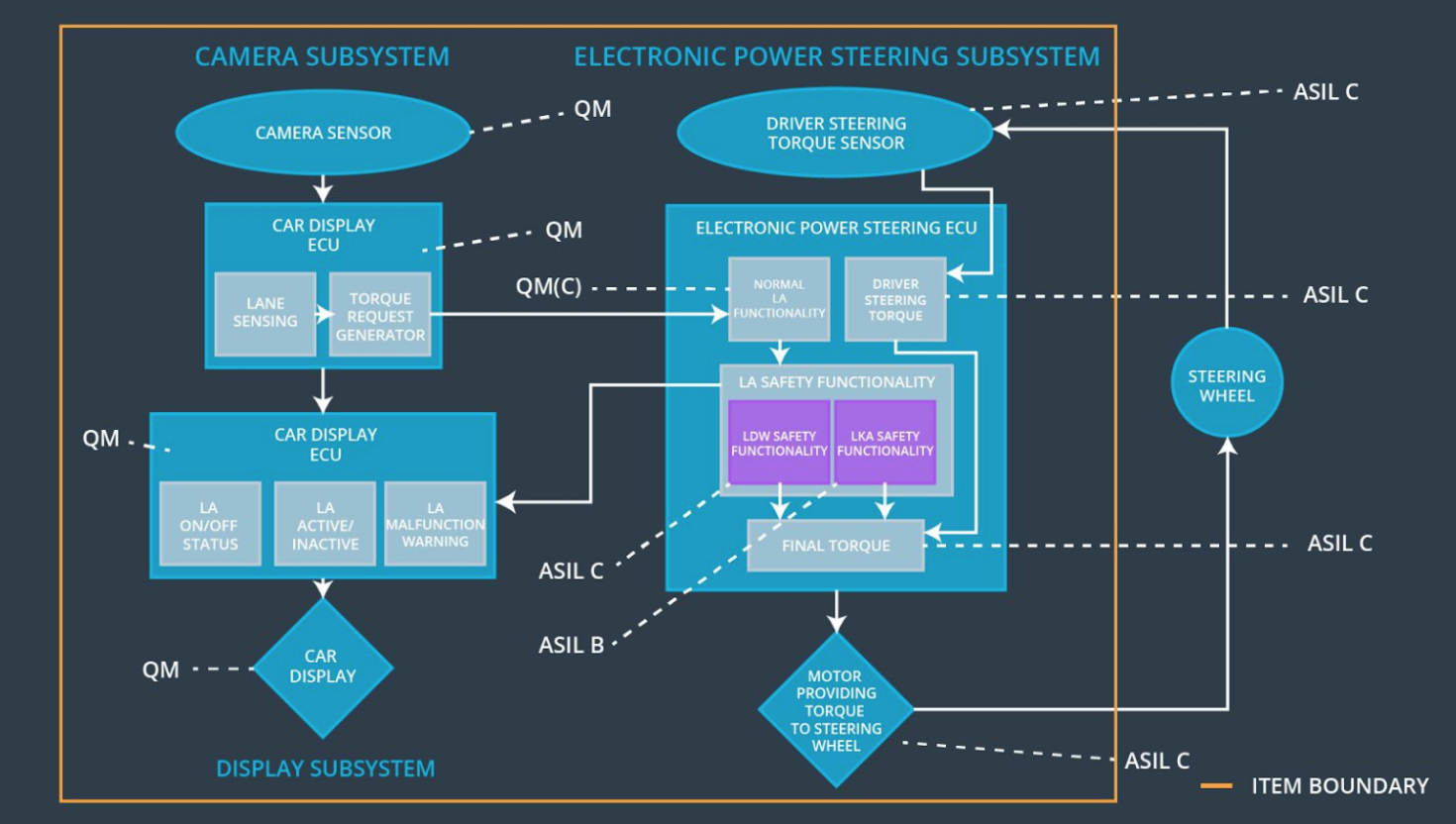
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

|  |  |  |
| --- | --- | --- |
| **ID** | **Validation Acceptance**  **Criteria and Method** | **Verification Acceptance**  **Criteria and Method** |
| Functional  Safety  Requirement  02-01 | Validate the choice of Max\_Duration does not mislead the driver into autonomous driving | Verify the system does be deactivated if the LKA function exceeds Max\_Duration |
| Functional  Safety  Requirement  02-02 | Validate the LKA shall be deactivated when camera cannot work properly (lane detection failed) | Verify the LKS does be deactivated if the camera cannot work properly |

## 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.]**

As shown below, the refined system architecture:



## 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude  is below Max\_Torque\_Amplitude |  |  |  |
| Functional  Safety  Requirement  01-02 | ﻿The lane keeping item shall ensure that the lane departure oscillating torque frequency  is below Max\_Torque\_Frequency |  |  |  |
| Functional  Safety  Requirement  02-01 | The steering ECU shall ensure that the wheel steering torque only be applied in the Max\_Duration |  |  |  |
| Functional  Safety  Requirement  02-02 | The LKA shall be deactivated when the Camera ECU outputs that the lane detection is failed |  |  |  |

## 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 | ﻿Turn off Lane  Assistant  functionality | ﻿Malfunction\_01 | Yes | Lane assistance malfunction warning on car display |
| WDC-02 | ﻿Turn off Lane  Assistant  functionality | ﻿Malfunction\_02 | Yes | Lane assistance malfunction warning on car display |
| WDC-03 | ﻿Turn off Lane  Assistant  functionality | ﻿Malfunction\_03 | Yes | Lane assistance malfunction warning on car display |