

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 |
| 01/05/19 | 1.0 | C.Wong | Initial Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 ultimate goal of functional safety is to avoid accidents by reducing risks to acceptable levels. The functional safety concept looks at items from a higher level, the system architectural design, and identifies what items (item architecture) affect safety. Safety goals are developed for those items, which then functional safety requirements can be derived.

# 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 oscillation torque by the LDW (Lane departure warning) function shall be limited. (ASIL C) |
| Safety\_Goal\_02 | The LKA (Lane keeping assistance) function shall limit steering torque to prevent sharp vehicle movements during rapid disengagement and engagement due to lane loss. (ASIL C) |

## 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 | Captures image and converts to pixel data sent to Camera Sensor ECU |
| Camera Sensor ECU | Receives pixel data from camera sensor, determines if vehicle is within target lane.  A status of whether the car is in or out of a lane is sent to the Car Display ECU and Power Steering ECU |
| Car Display | Displays a warning or status when it receives car display ECU data. |
| Car Display ECU | Receives status camera sensor ecu status and updates car display |
| Driver Steering Torque Sensor | Measures the torque applied by the driver and sends to the driver sterring torque subsystem |
| Electronic Power Steering ECU | Receives camera sensor ecu status and driver steering torque sensor data, calculates the torque and time duration needed for provide a haptic output/vibration to the steering wheel. |
| Motor | Receives commands from the Electronic Power Steering ECU and applies 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 | LDW function applies an oscillating steering torque that is above limit, i.e. too much |
| Malfunction\_02 | Lane Departure Warning (**LDW**) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | LDW function applies an oscillating steering torque that is unexpected. |
| Malfunction\_03 | Lane Keeping Assistance (**LKA**) function shall apply the steering torque when active in order to stay in ego lane | NO | LKA function disengages because camera ECU does not detect lane due to camera sensor intermittently seeing lane due to fog. |
| Malfunction\_04 | Lane Keeping Assistance (**LKA**) function shall apply the steering torque when active in order to stay in ego lane | WRONG | LKA function engages while driving backwards because the forward camera detects a lane and corrects for it. |

## 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 | (**LDW**) The electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 ms | Vibration/oscillating torque amplitude is set to zero. |
| Functional  Safety  Requirement  01-02 | (**LDW**) The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency | C | 50 ms | Vibration/oscillating torque frequency is set 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 | Define a reasonable limit for Max\_Torque\_Amplitude for LDW. | When the torque amplitude crosses the defined limit, system is turned off within the 50ms |
| Functional  Safety  Requirement  01-02 | Define a reasonable limit for Max\_Torque\_Frequency for LDW. | When the torque frequency crosses the defined limit, system is turned off within the 50ms |

**[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 LKA torque is applied for only Max\_Duration | C | 500 ms | LKA torque is set to zero. |
| Functional  Safety  Requirement  02-02 | The electronic power steering ECU shall ensure that the LKA torque is always zero while the vehicle is in reverse (moving backwards) | B | 500 ms | Function 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 | Set the reasonable value of Max\_Duration. | Verify that the system turns off if the LKA exceeds the Max\_Duration. |
| Functional  Safety  Requirement  02-02 | Set Reverse\_Mode\_Torque to TRUE. | Verify the system turns off if the LKA mode flag Reverse\_Mode\_Torque is set to TRUE |

## 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 | Electronic Power Steering ECU shall ensure that the lane departure torque amplitude shall not exceed Max\_Torque\_Amplitude. | **X** |  |  |
| Functional  Safety  Requirement  01-02 | Electronic Power Steering ECU shall ensure that the lane departure torque frequency shall not exceed Max\_Torque\_Frequency. | **X** |  |  |
| Functional  Safety  Requirement  02-01 | Electronic Power Steering ECU shall ensure that the LKA torque application is time limited for only Max\_Duration, | **X** |  |  |
| Functional  Safety  Requirement  02-02 | Electronic Power Steering ECU shall ensure that the LKA torque application is turned off if Reverse\_Mode\_Torque is TRUE | **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 | Off | If LDW Torque oscillation amplitude exceeds Max\_Torque\_Amplitude OR Torque oscillation frequency exceeds Max\_Torque\_Frequency | Yes | Warning light on the Car Display |
| WDC-02 | Off | If LKA torque applied for the duration longer than the Max\_Duration | Yes | Warning light on the Car Display |
| WDC-03 | Off | If vehicle transmission set to reverse, then Reverse\_Mode\_Torque is TRUE | Yes | Warning light on the Car Display |