

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

**Template Version 1.0, Released on 2018-06-29**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-6-29 | 1.0 | XU Kuangzheng | Initial version |
| 2018-6-29 | 2.0 | XU Kuangzheng | Second Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_Toc518029201)

[Table of Contents](#_Toc518029202)

[Purpose of the Functional Safety Concept](#_Toc518029203)

[Inputs to the Functional Safety Concept](#_Toc518029204)

[Safety goals from the Hazard Analysis and Risk Assessment](#_Toc518029205)

[Preliminary Architecture](#_Toc518029206)

[Description of architecture elements](#_Toc518029207)

[Functional Safety Concept](#_Toc518029208)

[Functional Safety Analysis](#_Toc518029209)

[Functional Safety Requirements](#_Toc518029210)

[Refinement of the System Architecture](#_Toc518029211)

[Allocation of Functional Safety Requirements to Architecture Elements](#_Toc518029212)

[Warning and Degradation Concept](#_Toc518029213)

# Purpose of the Functional Safety Concept

The purpose of a functional safety concept is to identify new requirements and allocate these requirements to system diagrams in a high level. It describes high-level performance requirements, addressing all issues identified from HARA.

In functional safety, "concept" is synonymous with "document". So the warning and degradation concept would be a document that discusses:

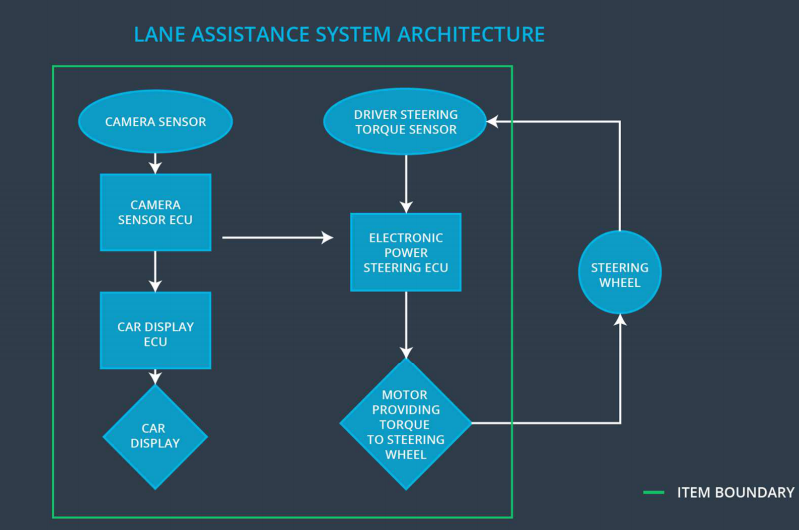
* How the driver will be warned of a malfunction.
* What the system will do to "degrade" the functionality i.e. take the system to a safe state and also recover from a safe state.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **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. |
| Safety\_Goal\_03 | Alert driver by other means (audible or visual) when LDW cannot detect lane lines. |
| Safety\_Goal\_04 | The LDW function shall deactivate when the camera sensor is unable to detect road markings, and shall warn the driver of its deactivation. |
| Safety\_Goal\_05 | The LKA system should check if the Electronic Power Steering ECU is functioning and give warning to driver if it stops working. |

## Preliminary Architecture



### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Camera device that retrieves images of the road in front of the vehicle. |
| Camera Sensor ECU | The camera sensor ECU identifies when the vehicle has accidentally departed its lane and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU. |
| Car Display | Graphic interface used to display the warning messages. |
| Car Display ECU | Processes input from camera subsystem and display the messages on the Car Display. |
| Driver Steering Torque Sensor | A sensor that measures that amount of effort the driver is making to steer the vehicle. This is important so that we do not interfere with intentional steering commands from the driver and impede his ability to control the vehicle. |
| Electronic Power Steering ECU | Vibrates the steering wheel when vehicle is drifting away from the current lane unintentionally. Add appropriate amount of torque based on feedback from torque sensor to keep vehicle in current lane. |
| Motor | Actuator used to apply requested 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

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

Lane Departure Warning (LDW) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | The electronic power steering subsystem shall ensure that the oscillating torque amplitude is less than Max\_Torque\_Amplitude | C | 50MS | Set LDW system torque 0 and visual indication |
| Functional  Safety  Requirement  01-02 | The electronic power steering subsystem  shall ensure that the oscillating torque frequency is less than Max\_Torque\_Frequency | C | 50MS | Set LDW system torque 0 and visual indication |

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 how drivers react to different torque amplitudes to prove that we chose an appropriate value | Verify that when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval |
| Functional  Safety  Requirement  01-02 | Test how drivers react to different torque amplitudes to prove that we chose an appropriate value | Verify that when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval |

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 torque is 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 | Confirm that the selected max\_duration dissuades drivers from taking their hands off the wheel. | Verify that the system really does turn off if the lane keeping assistance every exceeded Max\_Duration |

## Refinement of the System Architecture



## 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 electronic power steering ECU shall ensure that the oscillating torque amplitude is below Max\_Torque\_Amplitude | **√** |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the oscillating torque amplitude is below Max\_Torque\_Frequency | **√** |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration | **√** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Disable LDW  and alert | Oscillating torque frequency is higher than Max\_Torque\_Frequency or torque is higher than Max\_Torque\_Amplitude | YES | Driver indication of fault in LDW system |
| WDC-02 | Disable LKA  and alert | Lane keeping assistance torque is applied for more than Max\_Duration | YES | Driver indication of fault in LKA system |
| WDC-03 | Turn off functionality. | The lane departure warning function applies an oscillating torque with very high torque frequency (above limit). | Yes |  |