

Functional Safety Concept Lane Assistance

**Document Version: 0.1**

**Template Version 1.0, Released on 2017-06-21**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 3/3/18 | 0.1 | Ken Overholt | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Table of Contents

[Document history 2](#_Toc507858579)

[Table of Contents 2](#_Toc507858580)

[Purpose of the Functional Safety Concept 2](#_Toc507858581)

[Inputs to the Functional Safety Concept 3](#_Toc507858582)

[Safety goals from the Hazard Analysis and Risk Assessment 3](#_Toc507858583)

[Preliminary Architecture 4](#_Toc507858584)

[Description of architecture elements 4](#_Toc507858585)

[Functional Safety Concept 5](#_Toc507858586)

[Functional Safety Analysis 5](#_Toc507858587)

[Functional Safety Requirements 5](#_Toc507858588)

[Refinement of the System Architecture 7](#_Toc507858589)

[Allocation of Functional Safety Requirements to Architecture Elements 7](#_Toc507858590)

[Warning and Degradation Concept 8](#_Toc507858591)

# Purpose of the Functional Safety Concept

The safety goals are refined into functional safety requirements which are then allocated to the relevant parts of the system diagram where they will be implemented. This allocation may involve expanding the system architecture with new element blocks.

Next, the system architecture is refined to handle the new requirements. Each functional safety requirement will have the following attributed defined:

1. ASIL level
2. Fault tolerant time interval
3. Safe state

The purpose of the functional safety concept is to document all of this information.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The oscillating torque to the steering wheel 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 internal so that the driver cannot misuse the system for autonomous driving. |
| Safety\_Goal\_03 |  |
| Safety\_Goal\_04 |  |

## Preliminary Architecture

A close up of a sign

Description generated with high confidence

### 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 reads in images from the road. |
| 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 |  |
| Car Display ECU |  |
| Driver Steering Torque Sensor |  |
| Electronic Power Steering ECU |  |
| Motor |  |

# 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 ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50 ms | No torque is being applied |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscilating torque frequency is below Max\_Torque\_Frequency | C | 50 ms | No torque is being applied |

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 |  |  |
| Functional  Safety  Requirement  01-02 |  |  |

**[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 | 500 ms | No torque is being applied |

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 |  |  |

## 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.]**

A screenshot of a video game

Description generated with high confidence

## 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 the lane departure warning oscillating torque amplitude is below Max\_Torque\_Amplitude |  |  |  |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscilating torque frequency 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

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off the functionality | lane departure warning function applies an oscillating torque with very high torque frequency and amplitude | Yes | The owner’s manual will state that the feature will be turned off if it becomes too forceful. |
| WDC-02 | Turn off the functionality | Oscillating torque has reached the max\_duration value | Yes | The owner’s manual will state that the vehicle is not to be used for autonomous driving and that this feature will only be active for a short period before turning off. |