

Functional Safety Concept Lane Assistance

**Document Version: 1.1**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 3/3/18 | 0.1 | Ken Overholt | Initial draft |
| 3/7/18 | 0.2 | Ken Overholt | Candidate for final submission |
| 3/8/18 | 1.0 | Ken Overholt | Final Release |
| 3/9/18 | 1.1 | Ken Overholt | Second Release, updated the LKA Technical Safety Requirements to refer to the LKA component |
|  |  |  |  |

# Table of Contents

Table of Contents

[Document history 2](#_Toc508301744)

[Table of Contents 2](#_Toc508301745)

[Purpose of the Functional Safety Concept 3](#_Toc508301746)

[Inputs to the Functional Safety Concept 3](#_Toc508301747)

[Safety goals from the Hazard Analysis and Risk Assessment 3](#_Toc508301748)

[Preliminary Architecture 4](#_Toc508301749)

[Description of architecture elements 4](#_Toc508301750)

[Functional Safety Concept 5](#_Toc508301751)

[Functional Safety Analysis 5](#_Toc508301752)

[Functional Safety Requirements 6](#_Toc508301753)

[Refinement of the System Architecture 7](#_Toc508301754)

[Allocation of Functional Safety Requirements to Architecture Elements 8](#_Toc508301755)

[Warning and Degradation Concept 8](#_Toc508301756)

# 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. |

## Preliminary Architecture

A close up of a sign

Description generated with high confidence

### Description of architecture elements

|  |  |
| --- | --- |
| **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 torque request to the Electronic Power Steering ECU as well as sending a message to the Car Display ECU. |
| Car Display | The Car Display shows a sign in indicating the car has veered from its lane. |
| Car Display ECU | The Car Display ECU controls a light that tells the driver if the Lane Keeping system is on or off. It also controls a light that tells the driver that the Lane Departure Warning is activated. |
| Driver Steering Torque Sensor | The Driver Steering Torque Sensor detects how much the driver is turning the steering wheel, receive the torque request from the Camera subsystem, and add these two torque values together to output a final torque request to the motor. |
| Electronic Power Steering ECU | The Electronic Power Steering ECU controls the power steering system. |
| Motor | The motor receives the torque request from the Driver Steering Torque Sensor and moves 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

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | LDW torque output is set to 0 |
| Functional  Safety  Requirement  01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max\_Torque\_Frequency | C | 50 ms | LDW torque output 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 | Test how drivers react to different torque amplitudes and frequencies to prove that we chose an appropriate value. | Perform a software test inserting a fault into the system causing the Max\_Torque\_Amplitude value to cross the limit verify the torque drops to 0 and see what happens. |
| Functional  Safety  Requirement  01-02 | Test how drivers react to different torque amplitudes and frequencies to prove that we chose an appropriate value. | Perform a software test inserting a fault into the system causing the Max\_Torque\_Frequency value to cross the limit verify the torque drops to 0 and see what happens. |

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 | LKA 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 | Test and validate that the Max\_Duration chosen really did dissuade drivers from taking their hands off the wheel. | Verify that the system really does turn off if the lane keeping assistance exceeds 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 lane departure warning oscillating torque amplitude is below Max\_Torque\_Amplitude | **X** |  |  |
| 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 | **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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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. The driver will see a warning light on the dashboard when the system malfunctions. |
| 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. The driver will see a warning light on the dashboard when the lane keeping assistance is activated and it will disappear when not activated. |