

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 23AUG17 | 1.0 | Jim Reynolds | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

Document history 1

Table of Contents 2

Purpose of the Functional Safety Concept 2

Inputs to the Functional Safety Concept 3

Safety goals from the Hazard Analysis and Risk Assessment 3

Preliminary Architecture 3

Description of architecture elements 3

Functional Safety Concept 4

Functional Safety Analysis 4

Functional Safety Requirements 5

Refinement of the System Architecture 6

Allocation of Functional Safety Requirements to Architecture Elements 6

Warning and Degradation Concept 7

# Purpose of the Functional Safety Concept

The functional safety concept specifies the general (high-level) safety functionality of the item. It specifies the ASIL level, fault tolerant time interval and the safe state for each functional safety requirement.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The magnitude and frequency of the oscillating torque from the LDW shall be limited |
| Safety\_Goal\_02 | Continous activation of the LKA shall be prevented |
| Safety\_Goal\_03 | Steering angle and rate-of-change of steering angle of the LKA shall be limited as a function of the current vehicle speed |

## Preliminary Architecture

**The Lane Assistance System (LAS) consists of:**

* **Camera Sensor**
* **Camera Sensor ECU**
* **Car Display**
* **Car Display ECU**
* **Driver Steering Torque Sensor**
* **Electronic Power Steering ECU**
* **Motor**

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | A sensor that outputs an image of the scene in front of the vehicle |
| Camera Sensor ECU | A control module responsible for processing the camera sensor output, determine lane line position and trajectory, and requesting steering wheel torque for Lane Departure Warning (LDW) and Lane Keep Assistance (LKA) |
| Car Display | An actuator that displays information and messages to the driver via warning lamps or LCD display |
| Car Display ECU | A control module responsible for illuminating lamps or activating LCD display messages based on the LDW or LKA activation status |
| Driver Steering Torque Sensor | A sensor that outputs the torque that the driver is applying to the steering wheel |
| Electronic Power Steering ECU | A control module that is responsible for taking the driver steering torque signal, requested steering wheel torque from the camera sensor ECU, and the motor plant characterstics to create an actuator output signal to the motor that corresponds to the desired torque |
| Motor | An actuator that adds torque to the steering system in either direction (clockwise or counterclockwise) |

# 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 |  |  |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback |  |  |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane |  |  |

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

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 |  |  |  |  |

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.]**

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

## 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 |  |  |  |  |
| WDC-02 |  |  |  |  |