

Functional Safety Concept Lane Assistance

**Document Version: 1.0**

**Template Version 2.0, Released on 2017-10-17**



Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2017-10-16 | 1.0 | Daniel Gattringer | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Document History 2](#_Toc496104796)

[Table of Contents 2](#_Toc496104797)

[1. Purpose of the Functional Safety Concept 3](#_Toc496104798)

[2. Inputs to the Functional Safety Concept 3](#_Toc496104799)

[2.1. Safety goals from the Hazard Analysis and Risk Assessment 3](#_Toc496104800)

[2.2. Preliminary Architecture 3](#_Toc496104801)

[Description of architecture elements 3](#_Toc496104802)

[3. Functional Safety Concept 4](#_Toc496104803)

[3.1. Functional Safety Analysis 4](#_Toc496104804)

[3.2. Functional Safety Requirements 5](#_Toc496104805)

[3.3. Refinement of the System Architecture 6](#_Toc496104806)

[3.4. Allocation of Functional Safety Requirements to Architecture Elements 6](#_Toc496104807)

[3.5. Warning and Degradation Concept 7](#_Toc496104808)

# Purpose of the Functional Safety Concept

**[Instructions: Answer what is the purpose of a functional safety concept?]**

# 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 |  |
| Safety\_Goal\_02 |  |

## 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 |  |
| Camera Sensor 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

**[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 |  |  |
| 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 |  |  |  |  |

# 