

Functional Safety Concept Lane Assistance

**Document Version: Version 1.1, Released on 2018-11-21**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 11/18/18 | 1.0 | Emile Papillon | First draft |
| 11/21/18 | 1.1 | Emile Papillon | Review and release |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Document history

Table of Contents

Purpose of the Functional Safety Concept

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

Preliminary ArchitectureDescription of architecture elements

Functional Safety Concept

Functional Safety Analysis

Functional Safety Requirements

Refinement of the System Architecture

Allocation of Functional Safety Requirements to Architecture Elements

Warning and Degradation Concept

# Purpose of the Functional Safety Concept

The functional safety concept refines the safety goal and derives functional safety requirements. These requirements are then allocated to systems components in the systems diagram showing where each safety requirements will be implemented. The resulting architecture may differ from the preliminary architecture. Functional safety requirements are given the following attributees : ASIL level, Fault Tolerant Time Interval (FTTI) and the safe state.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

The following safety goals are the results of the Hazard and Risk Analysis (HARA) .

|  |  |
| --- | --- |
| **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 additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving. |
| Safety\_Goal\_03 | The lane assistance system shall turn off when the driver turns on the hazards. |
| Safety\_Goal\_04 | The lane warning feature shall be deactivated if the camera sensor has a fault. |

## Preliminary Architecture::Architecture_Diagrams:graphic_asset_2.pngDescription of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Responsible for detecting the lines |
| Camera Sensor ECU | Responsible of processing the data captured by the camera sensor and determining when the vehicle leaves the lane by mistake |
| Car Display | Interface with the human driver displaying system status and fault/malfunction warnings |
| Car Display ECU | Interface between the lane assistance system and the car display |
| Driver Steering Torque Sensor | Senses the torque input by the driver to provide just the right amount of extra torque for lane keeping assistance |
| Electronic Power Steering ECU | Interface between the driver torque sensor and the motor to calculate and apply the right amount of torque |
| Motor | Applies torque to the steering wheel/column. |

# 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 malfunctions and applies an oscillating torque with very high intensity (above expected level from human user). |
| 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. |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego | NO | The Lane Keeping Assistance function is not limited in time duration which lead to misuse |
| Malfunction\_04 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | WRONG | Lane keeping keeps applying lane centering torque while the driver is trying to pull off to shoulder |
| Malfunction\_05 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback. | WRONG | Malfunction in camera subsystem causes lane departure warning to trigger off at random moments |

## 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 Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50 ms | Vibration torque amplitude below Max\_Torque\_A mplitude. |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50 ms | Vibration frequency is below Max\_Torque\_Fr equency. |
| Functional  Safety  Requirement  01-03 | The Lane Keeping Feature shall turn off if a fault is detected in the camera subsystem | B | 50 ms | Lane Keeping Turns off when there is a fault in the camera subsystem |

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 | The chosen amplitude threshold Max\_Torque\_Amplitude is low enough to make the system safe. | Make sure that under no circumstances the system applied torque exceed Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The chosen frequency Max\_Torque\_Frequency is low enough to make the system safe | Make sure that under no circumstances the system rate of vibration exceeds Max\_Torque\_Frequency |
| Functional  Safety  Requirement  01-02 | Disabling the system every time there is a fault in the camera system ensures the safety of the user. | Introduce many different faults in the camera subsystem and make sure the LDW feature is disabled |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | The Lane Keeping Assistance shall be limited in time to a duration of Lane\_Keeping\_Timeout after which the feature turns off | B | 50 ms | Lane Keeping turns off after Lane\_Keeping\_Timeout |

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 | The duration Lane\_Keeping\_Timeout effectively makes the driver less likely to misuse the system | Make sure that in every possible use case the lane keeping does not exceed Lane\_Keeping\_Timeout seconds. |

## Refinement of the System Architecture::Architecture_Diagrams:graphic_asset_3.png

## 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 Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | **X** |  |  |
| Functional  Safety  Requirement  01-03 | The Lane Keeping Feature shall turn off if a fault is detected in the camera subsystem | **X** |  |  |
| Functional  Safety  Requirement  02-01 | The Lane Keeping Assistance shall be limited in time to a duration of Lane\_Keeping\_Timeout after which the feature turns off | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Turn off Lane Departure Warning functionality completely | Malfunction\_01, Malfunction\_02, Malfunction\_05 | Yes | LDW malfunction Warning light on Car Display |
| WDC-02 | Turn off Lane Keeping Assistance functionality  completely | Malfunction\_03, Malfunction\_04,  Malfunction\_05 | Yes | LKA malfunction Warning light on Car Display |