

Functional Safety Concept Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 10/9/2018 | 1.0 | John O’Shea | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Purpose of the Functional Safety Concept](#_fulgh8sf1ocg)

[Inputs to the Functional Safety Analysis](#_757cx6xm46zb)

[Safety goals from the Hazard Analysis and Risk Assessment](#_pi1c1upmo8jt)

[Preliminary Architecture](#_s0p6ihti6jgk)

[Description of architecture elements](#_cqb49updinx4)

[Functional Safety Concept](#_mx8us8onanqo)

[Functional Safety Analysis](#_mtn6qbhgsr36)

[Functional Safety Requirements](#_frlc9y84ede8)

[Refinement of the System Architecture](#_74udkdvf7nod)

[Allocation of Functional Safety Requirements to Architecture Elements](#_g2lqf7kmbspk)

[Warning and Degradation Concept](#_4w6r8buy4lrp)

# Purpose of the Functional Safety Concept

The purpose of the Functional Safety Concept is to performa a system level hazard analysis allocate safety requirements for each hazard. Technical Safety requirements are then derived from the system level safety requirements along with validation and verfication steps for each requirement.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The oscillating steering torque from the Lane Departure Warning (LDW) function shall be limited. |
| Safety\_Goal\_02 | The Lane Keeping Assistance (LKA) function shall be time limited such that the driver can take over control of the car to help try and avoid a hazard. |
| Safety\_Goal\_03 |  |
| Safety\_Goal\_04 |  |

## Preliminary Architecture

****

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures images of the road surface and sends them to the Camera Sensor ECU. |
| Camera Sensor ECU | - Validates the input data (CRC) from the sensor  - Processes the image to look for lane lines   * Makes a determination of a lane line violation * Alerts Car Display ECU with “Lane Departure Alert” message * Alerts Driver Steering Torque Sensor with “Lane Departure Alert” message |
| Car Display | Provides a visual indication to the driver if a “Lane Departure Alert ” was detected. |
| Car Display ECU | * Processes status packets from Camera Sensor ECU. * Detects “Lane Departure Alert” message packet and sets the Car Display warning indicator. * Detects “In Lane” message packet and sets the Car Display by turning off warning indicator |
| Driver Steering Torque Sensor | Measures the torque applied to the power steering unit. |
| Electronic Power Steering ECU | * Processes status packets from Drivier Steering Torque Sensor ECU. * Detects “Lane Departure Alert” message packet and sends a command to the motor to apply an oscillating torque to the drive power steering unit. * Detects “In Lane” message packet and send a reset command to disable the oscillating torque if enabled. |
| Motor | Monitors and applies commands from the Electronic Power Steering ECU to the steering 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 LDW function applies an oscillating torque with very high torque amplitude. |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | The LDW 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 lane | NO | The LKA function is not limited in time duration. |
| Malfunction\_04 |  |  |  |
| Malfunction\_05 |  |  |  |

## 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 LKA item shall ensure that the lane departure oscillating torque is below Max\_Torque\_Amplitude. | C | 50 ms | The torque amplitude is below Max\_Torque\_Amplitude |
| Functional  Safety  Requirement  01-02 | The LKA item shall ensure that the lane departure oscillating torque is below Max\_Torque\_Frequency. | C | 50 ms | The torque frequency is below Max\_Torque\_Frequency. |

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 | Apply LDW tests to validate the Max\_Torque\_Amplitude is high enough to alert the driver, but below an uncomfortable level that might cause loss of control. | Verify that the torque applied by the power steering ECU is disabled (0Nm) if the Max\_Torque\_Amplitude is exceeded. |
| Functional  Safety  Requirement  01-02 | Apply LDW tests to validate the Max\_Torque\_Frequency is high enough to alert the driver, but below an uncomfortable level that might cause loss of control. | Verify that the torque applied by the power steering ECU is disabled (0Nm)  if the Max\_Torque\_Frequency is exceeded. |
| Functional  Safety  Requirement  01-03 |  |  |

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 torque is applied only for Max\_Duration. | B | 500 ms | The torque applied by the power steering ECU after Max\_Duration is 0Nm. |

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 | Validate the Max\_Duration is long enough to alert the driver to take contol of the steering wheel | Verify that the LKA is disabled when Max\_Duration is reached. |
| Functional  Safety  Requirement  02-02 |  |  |

## 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 LKA shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The LKA shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | **X** |  |  |
| Functional  Safety  Requirement  01-03 |  |  |  |  |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the LKA torque is applied for Max\_Duration. | **X** |  |  |
| Functional  Safety  Requirement  02-02 |  |  |  |  |
|  |  |  |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | LDW is disabled | Malfunction\_01,  Malfunction\_02, | Yes | Car Display provides visual indication that LDW is disabled |
| WDC-02 | LKA is disabled | Malfunction\_03 | Yes | Car Display provides visual indication that LKA is disabled |