

Functional Safety Concept Lane Assistance

**Document Version: 1.0, Released 2018-07-01**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 07/01/2018 | 1.0 | Anand Mandapati | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 portion of the Safety Plan is to derive general hardware and software requirements that mitigate the identified risks in the electrical and electronic components that constitute the Lane Assistance System. The requirements are then allocated to the appropriate location in the system architecture. This could involve expanding the system architecture with new element blocks, if necessary.

# 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 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 interval so that the driver cannot misuse the system for autonomous driving. |

## Preliminary Architecture

### https://d17h27t6h515a5.cloudfront.net/topher/2017/July/5976a8f6_02-advanced-driver-assistance-system-architecture-01/02-advanced-driver-assistance-system-architecture-01.png

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Senses images of the road ahead of the vehicle. |
| Camera Sensor ECU | Detects lane lines on the images, derives position and direction of vehicle relative to the lane and generates torque request. |
| Car Display | Informs the driver about the state of the vehicle, including status and warnings of the LDW & LKA functions. |
| Car Display ECU | Process information for display to the driver. |
| Driver Steering Torque Sensor | Senses steering torque provided manually by the driver. |
| Electronic Power Steering ECU | Implements the logic behind both Lane Assistance System functions. Processes the inputs from the Camera Sensor ECU and Driver Steering Torque Sensor and controls the Motor that provides torque to the steering wheel. |
| Motor | Proivides torque to 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 lane keeping item shall ensure that the lane departure oscillation torque amplitude is below Max\_Torque\_Amplitude. | C | 50 ms | Reduce oscillating steering torque to zero |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillation torque frequency is below Max\_Torque\_Frequency. | C | 50 ms | Reduce oscillating steering torque to zero |

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 | Validate that Max\_Torque\_Amplitude is chosen high enough that the driver notices it but low enough not to cause loss of steering. | Verify that the system really sets oscillating torque to zero if the lane departure warning ever causes a vibration above Max\_Torque\_Amplitude. |
| Functional  Safety  Requirement  01-02 | Validate that Max\_Torque\_Frequency is chosen high enough that the driver notices it but low enough not to cause loss of steering. | Verify that the system really sets oscillating torque to zero if the lane departure warning ever causes a vibration above Max\_Torque\_Frequency. |

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 | Reduce augmented steering torque to zero. |

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 that the chosen amount for Max\_Duration really dissuades drivers from taking their hands off the wheel. | Verify that the system really sets the extra torque to zero if the Lane Keeping Assistance ever 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 oscillation torque amplitude is below Max\_Torque\_Amplitude. | **x** |  |  |
| Functional  Safety  Requirement  01-02 | The Electronic Power Steering ECU shall ensure that the lane departure oscillation 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 LDW function | The torque oscillation is above Max\_Torque\_Amplitude or Max\_Torque\_Frequency. | Yes, oscillating sttering torque reduced to zero | Warning on Car Display. |
| WDC-02 | Turn-off LKA function | The driver keeps hands off the wheel for longer than Max\_Duration | Yes, augmented steering torque set to zero. | Warning on Car Display. |