

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 |
| 28AUG17 | 1.1 | Jim Reynolds | WIP |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

Document history 1

Purpose of the Functional Safety Concept 2

Inputs to the Functional Safety Concept 2

Safety goals from the Hazard Analysis and Risk Assessment 2

Preliminary Architecture 3

Description of architecture elements 3

Functional Safety Concept 3

Functional Safety Analysis 4

Functional Safety Requirements 5

Refinement of the System Architecture 8

Allocation of Functional Safety Requirements to Architecture Elements 8

Warning and Degradation Concept 9

# 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 of the oscillating torque from the LDW shall be limited |
| Safety\_Goal\_02 | The frequency of the oscillating torque from the LDW shall be limited |
| Safety\_Goal\_03 | Continous activation of the LKA shall be prevented |
| Safety\_Goal\_04 | 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

### 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 | 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 |
| Malfunction\_04 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | MORE | The lane keeping assistance function applies a torque resulting in a steering angle too great for the vehicle speed (above limit) |
| Malfunction\_05 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | MORE | The lane keeping assistance function applies a torque resulting in a rate-of-change steering angle too great for the vehicle speed (above limit) |

## 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 oscillating torque amplitude is below Max\_Torque\_Amplitude | C | 50ms | Lane keeping item output torque = 0 |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Frequency | C | 50ms | Lane keeping item output torque = 0 |

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 | Criteria  100% of drivers are able to regain steering control  Event  Manual override of requested torque at limit (with buffer)  1.2 \* Max\_Torque\_Amplitude  1.0 \* Max\_Torque\_Frequency  Method  Vehicle on test track with driving coaches and various drivers | Criteria  Lane\_Keep\_Torque = 0 within 50ms of event  Event  Fault injection by RAM address write, requested torque amplitude exceeds limit  Method  Hardware-in-the-loop verification |
| Functional  Safety  Requirement  01-02 | Criteria  100% of drivers are able to regain steering control  Event  Manual override of requested torque at limit (with buffer)  1.0 \* Max\_Torque\_Amplitude  1.2 \* Max\_Torque\_Frequency  Method  Vehicle on test track with driving coaches and various drivers | Criteria  Lane\_Keep\_Torque = 0 within 50ms of event  Event  Fault injection by RAM address write, requested torque frequency exceeds limit  Method  Hardware-in-the-loop verification |

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 | 500ms | Lane keeping item output torque = 0 |
| Functional  Safety  Requirement  02-02 | The lane keeping item shall ensure that the total absolute steering angle does not exceed Max\_Steering\_Angle(Vehicle\_Speed) | C | 50ms | Lane keeping item output torque = 0 |
| Functional  Safety  Requirement  02-03 | The lane keeping item shall ensure that the rate-of-change of steering angle does not exceed Max\_Steering\_Rate(Vehicle\_Speed) | C | 50ms | Lane keeping item output torque = 0 |

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 | Criteria  100% of drivers are able to regain steering control  Event  Driver removes hands from wheel with system active, retakes control after system is disabled by functional safety feature  Method  Vehicle on test track with driving coaches and various drivers | Criteria  Lane\_Keep\_Torque = 0 within 500ms of event  Event  Fault injection by RAM address write, requested lane keep assistance torque remains active indefinitely  Method  Hardware-in-the-loop verification |
| Functional  Safety  Requirement  02-02 | Criteria  No loss of traction, all wheels remain on the ground  Event  Manual override of requested torque at limit (with buffer)  1.2 \* Max\_Steering\_Angle(Vehicle\_Speed)  Method  Vehicle on test track, unmanned, remotely controlled due to rollover risk | Criteria  Lane\_Keep\_Torque = 0 within 50ms of event  Event  Fault injection by RAM address write, requested steering angle exceeds limit  Method  Hardware-in-the-loop verification |
| Functional  Safety  Requirement  02-03 | Criteria  No loss of traction, all wheels remain on the ground  Event  Manual override of requested torque at limit (with buffer)  1.2 \* Max\_Steering\_Rate(Vehicle\_Speed)  Method  Vehicle on test track, unmanned, remotely controlled due to rollover risk | Criteria  Lane\_Keep\_Torque = 0 within 50ms of event  Event  Fault injection by RAM address write, requested rate-of-change of steering angle exceeds limit  Method  Hardware-in-the-loop verification |

## 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude | **X** |  |  |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude 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** |  |  |
| Functional  Safety  Requirement  02-02 | The lane keeping item shall ensure that the total absolute steering angle does not exceed Max\_Steering\_Angle(Vehicle\_Speed) | **X** |  |  |
| Functional  Safety  Requirement  02-03 | The lane keeping item shall ensure that the rate-of-change of steering angle does not exceed Max\_Steering\_Rate(Vehicle\_Speed) | **X** |  |  |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | System disabled until module reset | Malfunction\_01 | Yes, immediately | 1. Audible Chime  2. Pop-up message on instrument cluster |
| WDC-02 | System disabled until module reset | Malfunction\_02 | Yes, immediately | 1. Audible Chime  2. Pop-up message on instrument cluster |
| WDC-03 | System disabled until module reset | Malfunction\_03 | Yes, immediately | 1. Audible Chime  2. Pop-up message on instrument cluster |
| WDC-04 | System disabled until module reset | Malfunction\_04 | Yes, immediately | 1. Audible Chime  2. Pop-up message on instrument cluster |
| WDC-05 | System disabled until module reset | Malfunction\_05 | Yes, immediately | 1. Audible Chime  2. Pop-up message on instrument cluster |