

Functional Safety Concept Lane Assistance

**Document Version: 1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 12.01.2019 | 1.0 | Michael Ikemann | Initial definition of functional safety |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 define the single functionalities from a high level perspective, how the the safety can be ensured as much as possible for each of it’s features and the functionality’s ASIL level.**

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

|  |  |
| --- | --- |
| **ID** | **Safety Goal** |
| Safety\_Goal\_01 | The vehicle should detect bad weather conditions and inform the other that the system’s functionality might be limited and/or should automatically be disabled after informing the user in cases where for example the sensors are covered by snow and not fully functional. |
| Safety\_Goal\_02 | The vibration of the steering while should be limited in all involved components to prevent accidents caused by a scared driver. |
| Safety\_Goal\_03 | If the user removes the hands from the steering wheel the driver should be informed audiovisual that the lane guidance will be deactivated because the system shall not be used in an autonomous manner. |
| Safety\_Goal\_04 | It shall be verified that the lane guidance system will be disabled when the vehicle is not driving. |

## Preliminary Architecture

### https://d17h27t6h515a5.cloudfront.net/topher/2017/July/5976aa23_02-advanced-driver-assistance-system-architecture-02-1/02-advanced-driver-assistance-system-architecture-02-1.png

### Description of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Captures the image. Is mounted at the top of the wind screen. |
| Camera Sensor ECU | Analyses the image – detects the lane and the detection certainty and decides if the user shall be warned about lane departure or follow the center of the lane if lane guidance is activated. |
| Car Display | Visualizes if lane guidance and departure features are activated and also informs the user when a lane departure occurs. |
| Car Display ECU | Is responsible for the visualization of the car’s dashboard. Needs to be extended for the visualization of LGA related features. |
| Driver Steering Torque Sensor | Detects with which amount of force the driver tries to steer. In case of the LGA a non-existing steering of the driver in a curve should lead to a warning so the driver will not use the LGA in an autonomous way. Also a counter-steering of the driver should be detected and disable the lane guide so the driver will regain control of the vehicle if required. |
| Electronic Power Steering ECU | The EPS ECU decides by the information provided by the DSTS and CS ECU which amount of torque to apply to the steering wheel. |
| Motor | Applies the amount of torque provided by the EPS ECU to the steering wheel so that the vehicle will (for example) follow the lane detected. |

# 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 | The lane departure warning applies more oscillating torque than intended. | A too strong vibration of the steering wheel would distract the driver. |
| Malfunction\_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | The computation of the camera ECU arrives too late at the EPS ECU. | The driver will be notified too late to still be able to react due to a delayed notification. |
| Malfunction\_03 | Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane | The LKA steers wrongly within a road work site due to crossing lane markers which irritated the CS ESU. | The vehicle drives into a wrong direction and potentially causes an accident. |

## Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | Bad weather conditions and incorrectly working sensors are detected and the user will be informed. | B | 0.1 | The system will be disabled and the user will be informed about it’s state. |
| Functional  Safety  Requirement  01-02 | The detection data is provided in intervals of 10 Hz. In case of lost messages the system will automatically be disabled. | B | 0.1s | The user will be informed that the system works incorrectly and the LDW will be disabled and it’s status shown in the dash board. |

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 vehicle will be tested under several weather conditions and the sensors intentionally blocked. | When ever a sensor can not guarantee it’s correct functionality anymore due to crosschecks with other sensors the system automatically gets disabled. |
| Functional  Safety  Requirement  01-02 | The receiving units verify that status updates from the CS ECU arrive in the correct order in time intervals of 10 Hz.  The CRC checksum computed at the receiver matches the provided checksum. | The communication will intentionally be disturbed and the CS disabled. The system should be automatically disabled when status updates due not arrive in time. |

Lane Keeping Assistance (LKA) Requirements:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  02-01 | If the current situation can be detected reliably anymore the system should slow down the car and instantly inform the driver. | B | 0.1 | The LKA is disabled and the user informed via the dashboard and a warning signal in the dashboard |

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 | In situations where it can not clearly detect the correct lanes anymore such as in road work sites it should temporarily be disabled. | The car is tested in several different situations and correctly informs the user when it can not reliably support the lane guidance. |

## 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 | Bad weather conditions and incorrectly working sensors are detected and the user will be informed. |  | **Detects sensor failures in disables the LDW.** | **Informs the driver that the LDW has been disabled.** |
| Functional  Safety  Requirement  01-02 | The detection data is provided in intervals of 10 Hz. In case of lost messages the system will automatically be disabled. | **Detects incorrect transmissions** |  | **Informs the driver that the LDW has been disabled.** |
| Functional  Safety  Requirement  02-01 | In situations where it can not clearly detect the correct lanes anymore such as in road work sites it should temporarily be disabled |  | **Automatically detects uncertain situations and stops taking control if it could lead to an accident.** | **Informs the driver that the LKA does not support at the moment.** |

## Warning and Degradation Concept

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
| WDC-01 | Disabled until next motor start. | CRC checksum errors in communication and or no data provided at 10 Hz rate as required. | LDW disabled. | Error light in dashboard. |
| WDC-02 | Disabled temporarily till situation is safe again. | Too many, none or contradictionary lanes detected. | LKA temporarily disabled. | Inactivity visualized in dashboard. |