Elektrobit

UDACITY

# Functional Safety Concept Lane Assistance

**Document Version:** [Version]

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

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 27.02.2020 | 1.0 | Uwe Ehmann | Initial document |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Functional Safety Concept

A vehicle level functional safety concept defines a system architecture to ensure the safety goals. From the safety goals which are the result of the hazard and risk analysis, higher level safety requirements are derived and allocated to the system architecture.

# Inputs to the Functional Safety Concept

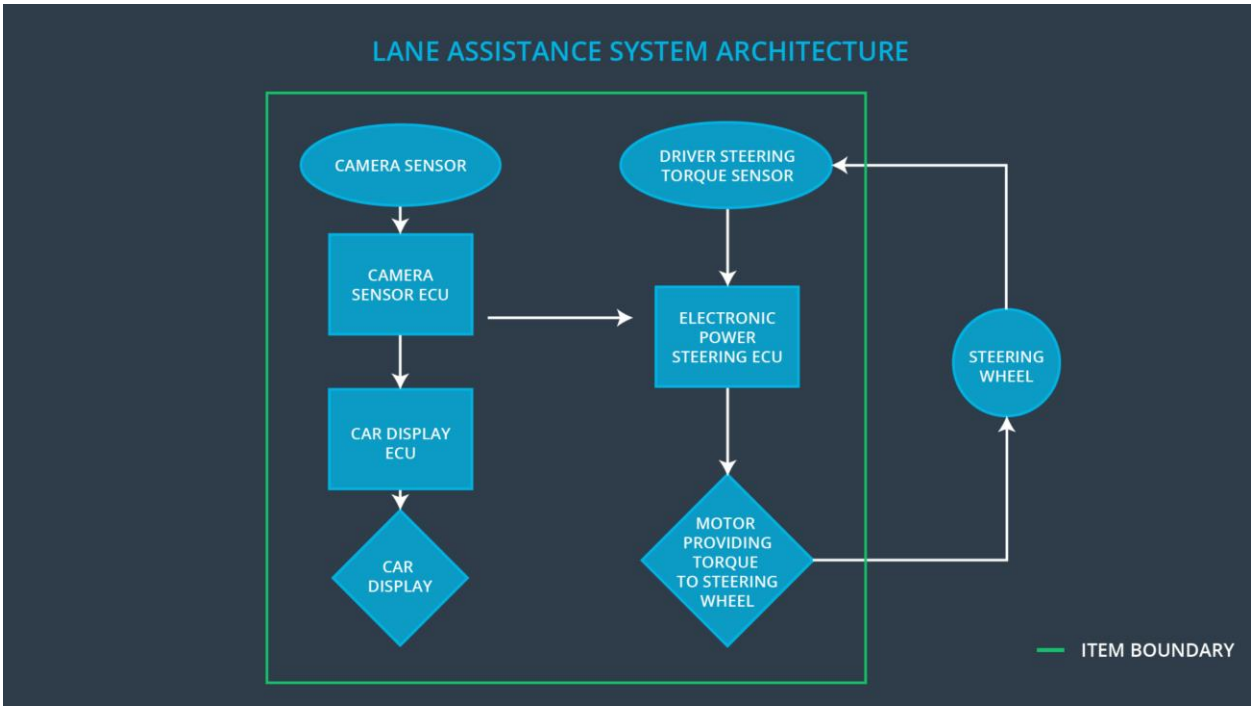
## Safety goals from the Hazard Analysis and Risk Assessment]

| 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

The item boundary was drawn to include three sub-systems:

- Camera system
- Electronic Power Steering system
- Car Display system




## Description of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | Provides environment images to the camera ECU. |
| Camera Sensor ECU | Detects the lane lines and their relative position to the car. |
| Car Display | Displays a lane departure warning. |
| Car Display ECU | Processes signal form the camera ECU and the Electronic Power Steering ECU in order to trigger warning symbols on the display. |
| Driver Steering Torque Sensor | Measures the steering torque of the driver and provides it to the Electronic Power Steering ECU. |
| Electronic Power Steering ECU | Takes signals from the sensor ECUs and derives a steering torque to be applied. |
| Motor | Applies the actual requested steering torque from the Electronic Power Steering ECU 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 oscillating torque amplitude is below MAX_TORQUE_AMPLITUDE. | C | 50 ms | LDW torque request amplitude is set to zero. |
| Functional Safety Requirement 01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below MAX_TORQUE_FREQUENCY. | C | 50 ms | LDW torque request frequency is set 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 | MAX_TORQUE_AMPLITUDE must be chosen to be high enough to be recognized by the and low enough to not cause loss of steering. | Verify that the system turns off if MAX_TORQUE_TORQUE is exceeded. |
| Functional Safety Requirement 01-02 | MAX_TORQUE_FREQUENCY must be chosen to be high enough to be recognized by the and low enough to not cause loss of steering. | Verify that the system turns off if MAX_TORQUE_ FREQUENCY is exceeded. |

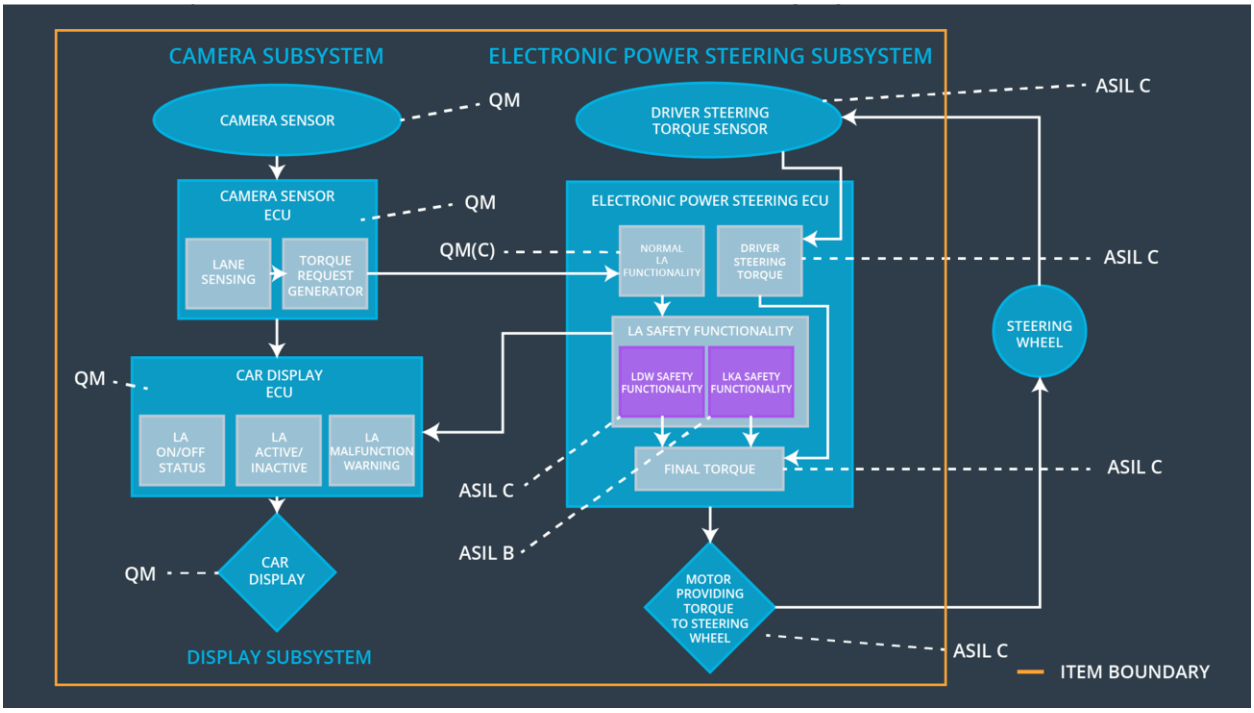
Lane Keeping Assistance (LKA) Requirements:

| 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 | LKA torque request is set 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 | MAX_DURATION must be chosen to be long enough to ensure an overall effect of the function and short enough to not be misused as L3 function. | Verify that the system turns off after 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 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 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 functionality | Malfunction_01<br>Malfunction_02 | Yes | The car display signals degraded functionality |
| WDC-02 | Turn off functionality | Malfunction_03 | Yes | The car display signals degraded functionality |