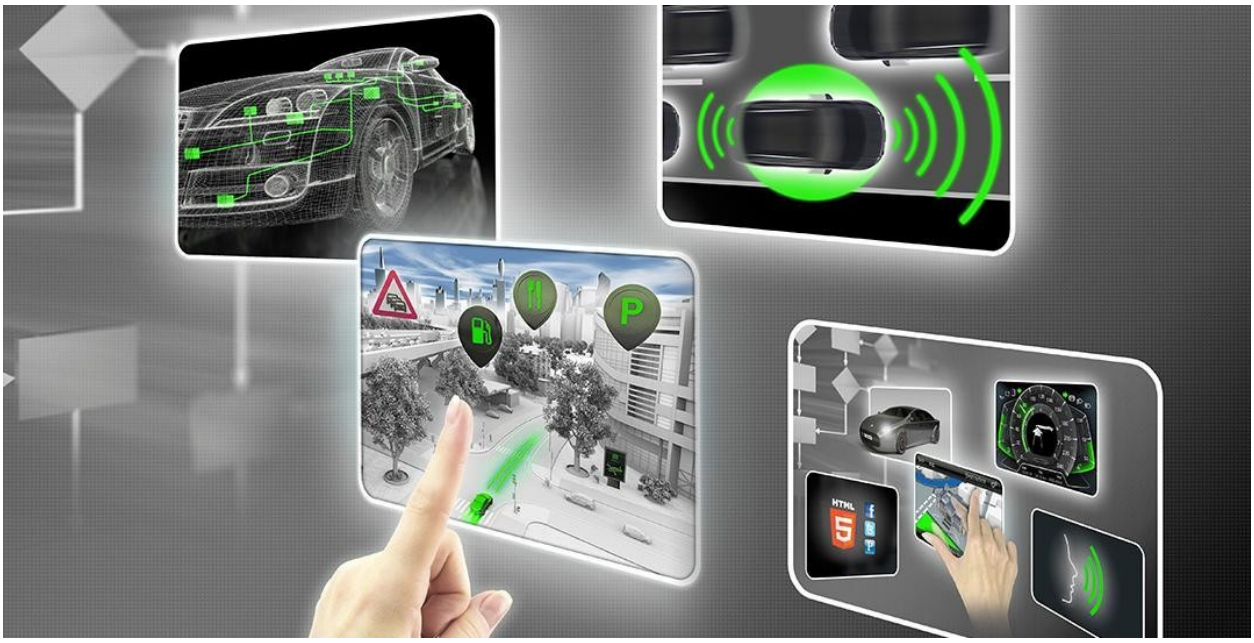
Elektrobit

UDACITY

# Functional Safety Concept Lane Assistance

**Document Version:1.0**

Template Version 1.0, Released on 2017-06-21



# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 21.08.2017 | 1.0 | Y.Wiyogo | Initial document |
| 23.08.2017 | 1.1 | Y.Wiyogo | Complete the functional safety concept tables |
| 24.08.2017 | 1.2 | Y.Wiyogo | Update paragraph position |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Functional Safety Concept

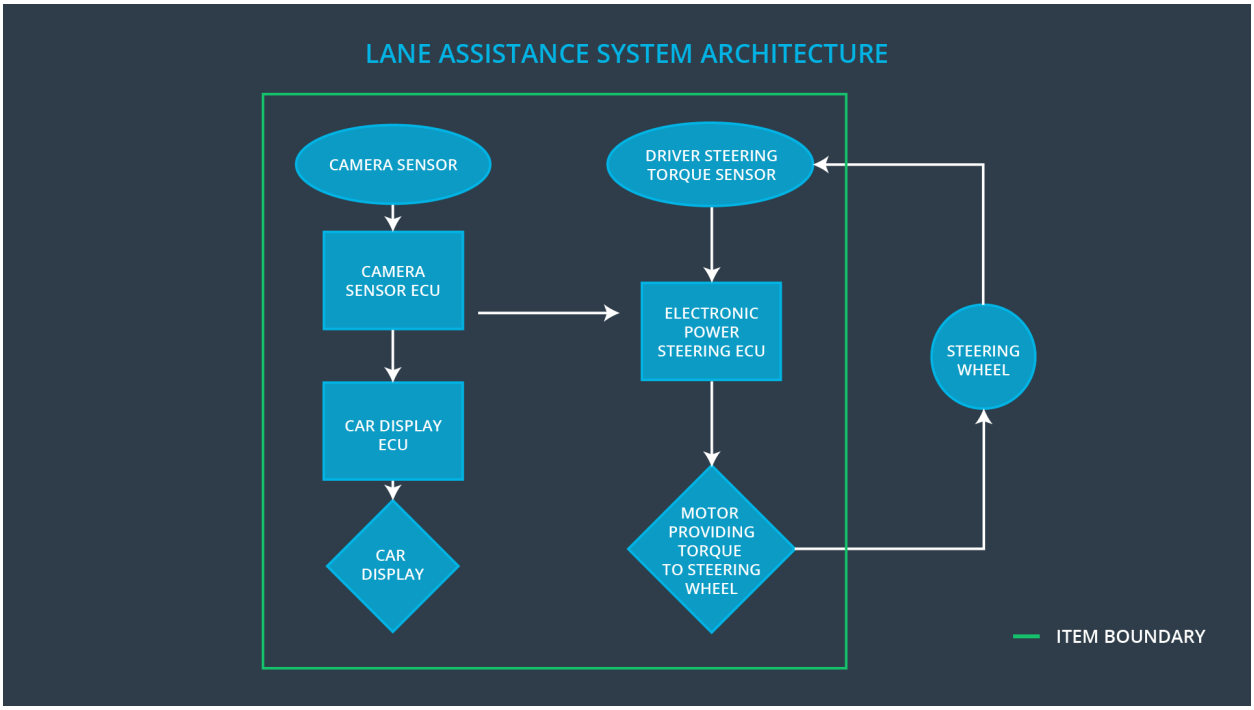
The purpose of the functional safety concept is to describe the implementation of the independent safety solutions for a defined item.

# 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 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 a autonomous driving. |
| Safety_Goal_03 | The lane detection shall not be activated if the detection for a certain environment is not reliable. |
| Safety_Goal_04 | A sudden strong torque shall be avoided. |

## Preliminary Architecture



Description of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | A sensor for aquiring environment information as image. |
| Camera Sensor ECU | A processor chip for processing the acquired image data. |
| Car Display | A display device  for visualizing the activation of the function to the driver. |
| Car Display ECU | A processor chip for processing the data from the camera sensor ECU |
| Driver Steering Torque Sensor | A sensor that acquires the torque value of the steering wheel |
| Electronic Power Steering ECU | A processor chip for processing data from camera sensor ECU and torque sensor. |
| Motor | An electric motor that interpret the EPS ECU data to control 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 | MORE | The lane departure warning function applies an oscillating torque with very high torque **amplitude** (above limit) |

| | | | |
|---|---|---|---|
| | feedback | | |
| 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 amplidute is below Max_Torque_Amplitude | C | 50 ms | Turn off LDW |
| 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 | Turn off LDW |

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Functional Safety Requirement | Set oscillating torque amplitude to Max_Torque_Amplitude causes the light warning to be turned on | when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant |

| | | |
|---|---|---|
| 01-01 | | time interval |
| Functional Safety Requirement 01-02 | Set oscillating torque frequency to Max_Torque_Frequency causes the warning light to be turned on | when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval |

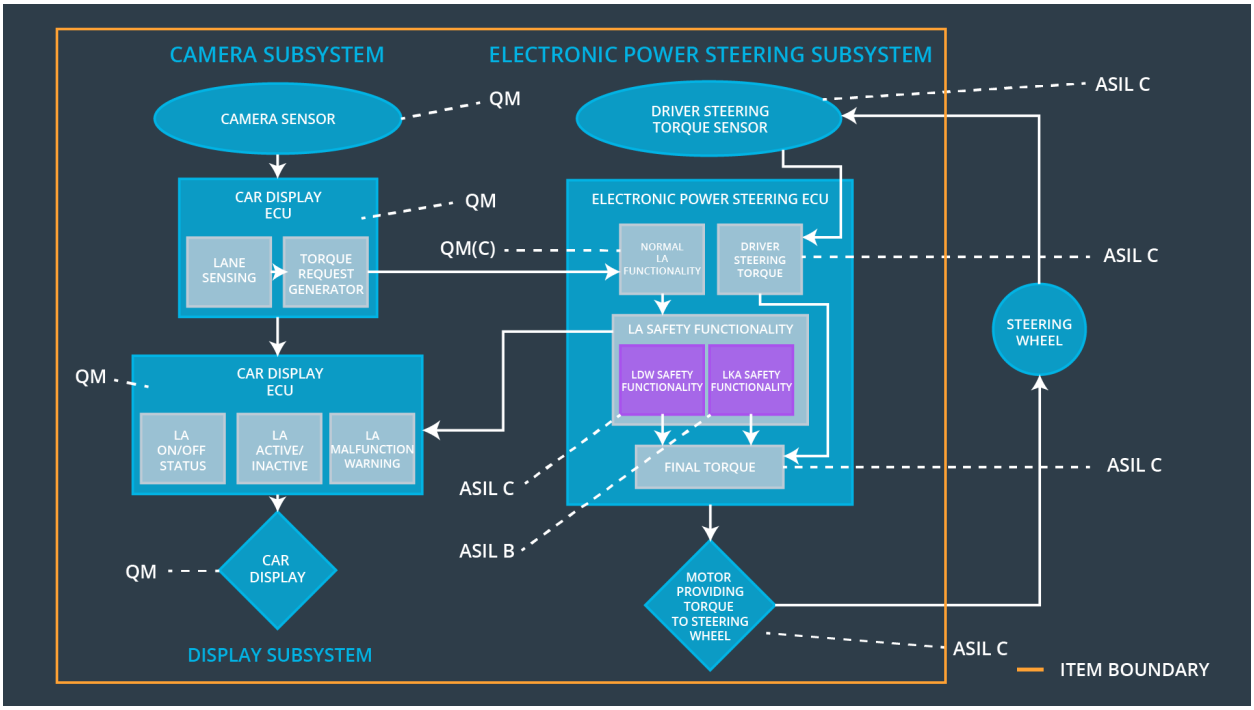
Lane Keeping Assistance (LKA) Requirements:

| 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. | D | 500 ms | Turn off LKA |

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 | Let the LKA active until the Max_Duration, and the warning light has to be turned on | when the time duration exceeds the limit, the lane assistance output is set to zero within the 500 ms fault tolerant time interval |

# 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 amplidute 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 the function | Is_Max_Torque_ Exceeded | Yes | Turn on warning light on car display |
| WDC-02 | turn off the function | Is_Max_Duration _Exceeded | Yes | Turn on warning light on car display |