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 |
|---|---|---|---|
| 1/2/2018 | 1.0 | Joshua Schoenfield | First Attempt |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents



# Purpose of the Functional Safety Concept

The functional safety concept is a document that looks at the general functionality of the Lane Assistance Item and identifies high level safety goals. It then refines those high level safety goals into specific functional safety requirements. It then allocates those functional safety goals to specific parts of the item's architecture.

The functional safety concept consists of:
- Functional safety analysis
- Functional safety requirements
- Functional safety architecture
- Warning and degradation concept

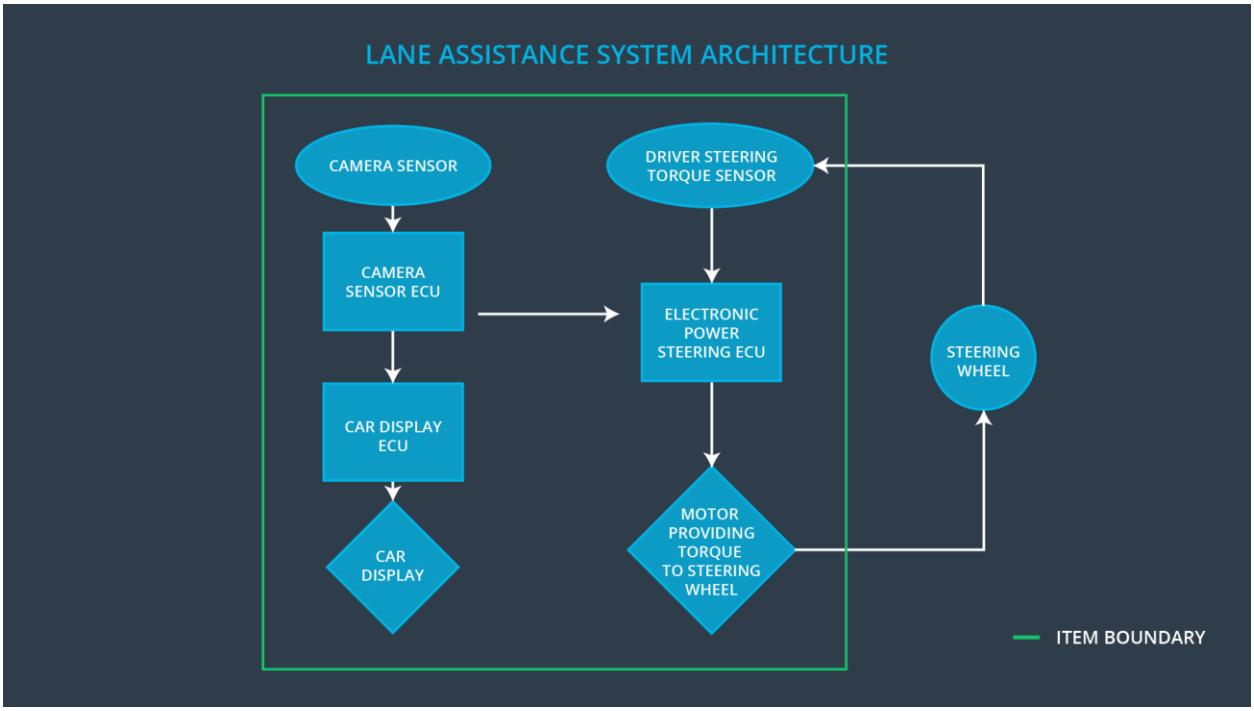
# Inputs to the Functional Safety Concept

## 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 architecture of the item can be seen in the following diagram:




### Description of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | The camera sensor reads in images from the road and reports these images to the Camera Sensor ECU |
| Camera Sensor ECU | The camera sensor ECU identifies when the vehicle has accidentally departed its lanes and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU |
| Car Display | The Car Display visually presents information to the Driver |
| Car Display ECU | The Car Display ECU accepts information about the car's position in the lane from the Camera Sensor ECU and renders it for display to the driver by the Car Display |
| Driver Steering Torque Sensor | The driver steering torque sensor reads what torque is being applied by the driver to the steering wheel, and communicates that to the Electronic Power Steering ECU |
| Electronic Power Steering ECU | The Electronic Power Steering ECU calculates what additional torque should be applied to the steering wheel based off of the cars position in the lane (as determined by the Camera Sensor ECU) and the torque being applied to the steering wheel by the driver as determined by the Driver Steering Torque Sensor |
| Motor | The Motor applies the additional torque requested by 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 electronic power steering ECU **shall** ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude | C | 50 ms | Lane assistance output is set to zero |
| Functional | The electronic power steering ECU **shall** | C | 50 ms | Lane assistance |

| | | | | |
|---|---|---|---|---|
| Safety Requirement 01-02 | ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | | | output 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 | Test how drivers react to different torque amplitudes to validate the choice of Max_Torque_Amplitude, ensuring that at that value the driver is able to control the vehicle. | When the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval |
| Functional Safety Requirement 01-02 | Test how drivers react to different torque frequencies to validate the choice of Max_Torque_Frequency, ensuring that at that value the driver is able to control the vehicle. | When the torque amplitude 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 | B | 500 ms | Lane assistance output is set to zero |

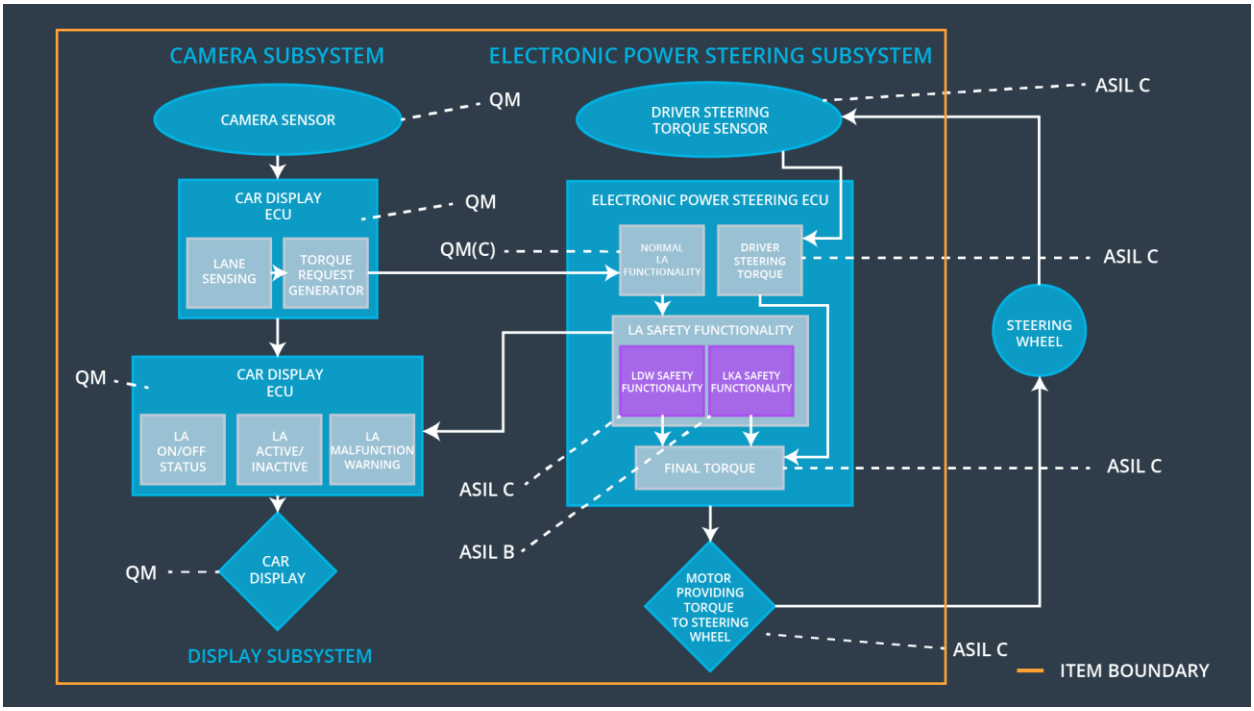
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|

| | | |
|---|---|---|
| Functional Safety Requirement 02-01 | Test that the value of Max_Duration chosen to validate that it dissuades drivers from taking their hands off the wheel. | Verify that the system really does turn off within 500 ms if the lane keeping assistance ever exceeds Max_Duration |

## Refinement of the System Architecture

The refined system architecture, including all the ASIL labels can be seen in the following figure:




## 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 oscillating torque amplitude is below Max_Torque_Amplitude | ✓ | | |

| | | | | |
|---|---|---|---|---|
| Functional Safety Requirement 01-02 | The Electronic Power Steering ECU **shall** ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | ✓ | | |
| Functional Safety Requirement 02-01 | The Electronic Power Steering ECU **shall** ensure that the lane keeping assistance torque is applied for only Max_Duration | ✓ | | |

## Warning and Degradation Concept

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | LDW System Turns Off | Malfunction_01 or Malfunction_02 | Yes | Lane Assistance Malfunction Warning Appears on Car Display |
| WDC-02 | LKA System Turns Off | Malfunction_03 | Yes | Lane Assistance Malfunction Warning Appears on Car Display |