Elektrobit

UDACITY

# Functional Safety Concept Lane Assistance

**Document Version: 1.0**
**Released on 2017-09-06**

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 2017-09-06 | 1.0 | Yifei Li | First Submission |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Functional Safety Concept

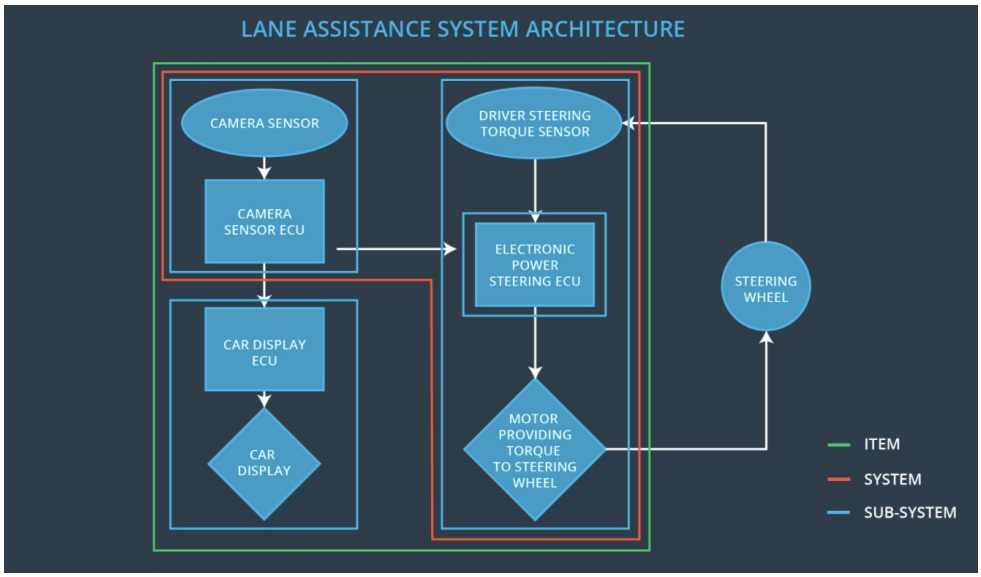
The purpose of Functional Safety Concept is to document functional safety goals and define its corresponding functional safety requirements at the product concept phase so that the system is designed to be functional safe and risks can be avoided and the reduced to acceptable levels.

# 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



### Description of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | Detect road in front of the car and transform it into digital pixels and a streamline of digital information for camera sensor ECU to process |
| Camera Sensor ECU | Process raw images from camera sensor for lane identification and generate torque request to electronic power steering ECU |
| Car Display | A LCD or LED panel that display human interpretable information (lane assistance on/off and lane assistance active/inactive) |
| Car Display ECU | Process and and transmit the data to right format that is readable by car display |
| Driver Steering Torque Sensor | Detect torque applied and convert it to digital information |
| Electronic Power Steering ECU | Receive torque request from camera sensor ECU and analyze the torque applied by driver and process it to motor in order to adjust the steering wheel to maintain the car inside the lane |
| Motor | Applied torque to mechanical components |

# 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 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 | 50ms | Lane departure system is turned off |
| Functional Safety Requirement 01-02 | The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | C | 50ms | Lane departure system is turned off |

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 | Departure warning vibrates the steering wheel at the specified amplitude | Departure warning vibrates the steering wheel is neither too high for driver to handle or too low that the driver cannot feel the vibration |
| Functional Safety Requirement 01-02 | Departure warning vibrates the steering wheel at the specified frequency | Departure warning vibrates the steering wheel is neither too high for driver to handle or too low that the driver cannot feel the vibration |

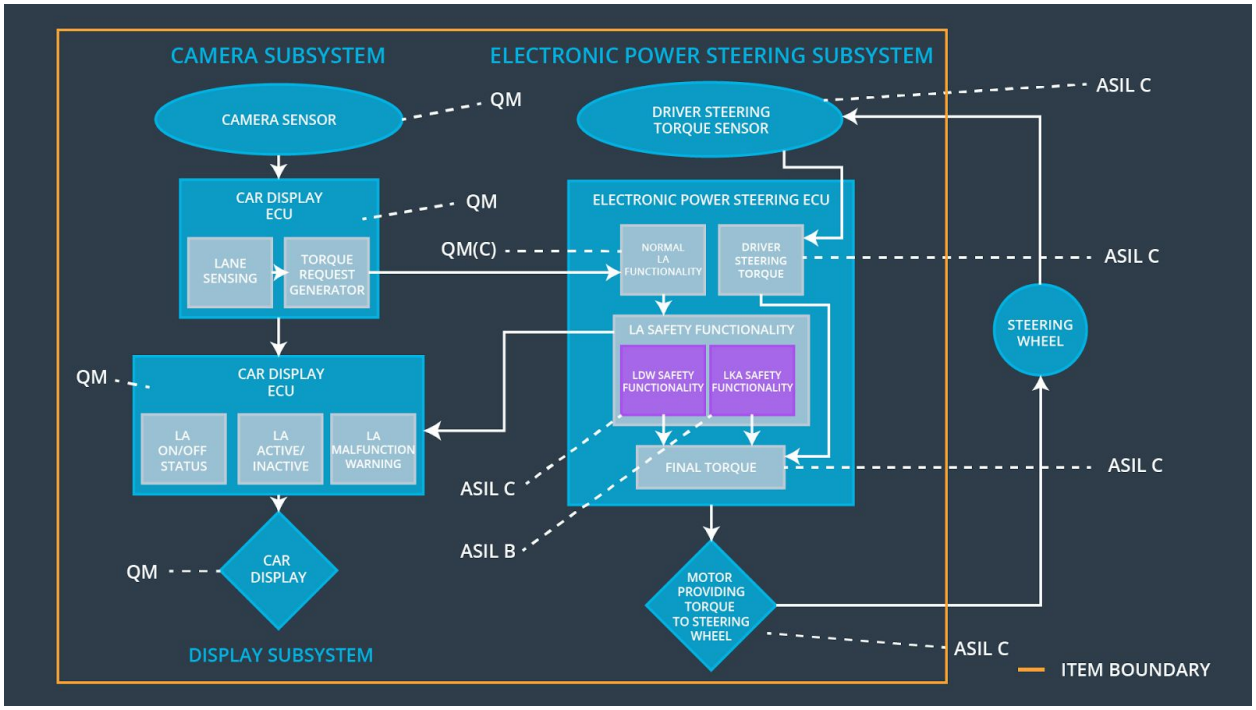
Lane Keeping Assistance (LKA) Requirements:

| 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 assistance system is turned off |

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 | Lane keeping assistance applied specified torque to the actuator | Lane keeping assistance applied neither too high for a driver to handle nor too low torque that not enough to move car back to the lane |

# 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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude | **x** | | |
| Functional Safety Requirement 01-02 | The electronic power steering ECU 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 | Lane departure warning output is set to zero | Oscillating torque amplitude greater than Max_Torque_Ampltidue | Yes | Warning messages displayed on car display |
| WDC-02 | Lane departure warning output is set to zero | Oscillating torque frequency greater than Max_Torque_Frequency | Yes | Warning messages displayed on car display |
| WDC-03 | Lane keeping assistance output is set to zero | Fault Tolerant Time Interval > 500ms | Yes | Warning messages displayed on car display |