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 |
|---|---|---|---|
| 6/2/2018 | 1.0 | Tariq Rafique | Complete |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Functional Safety Concept

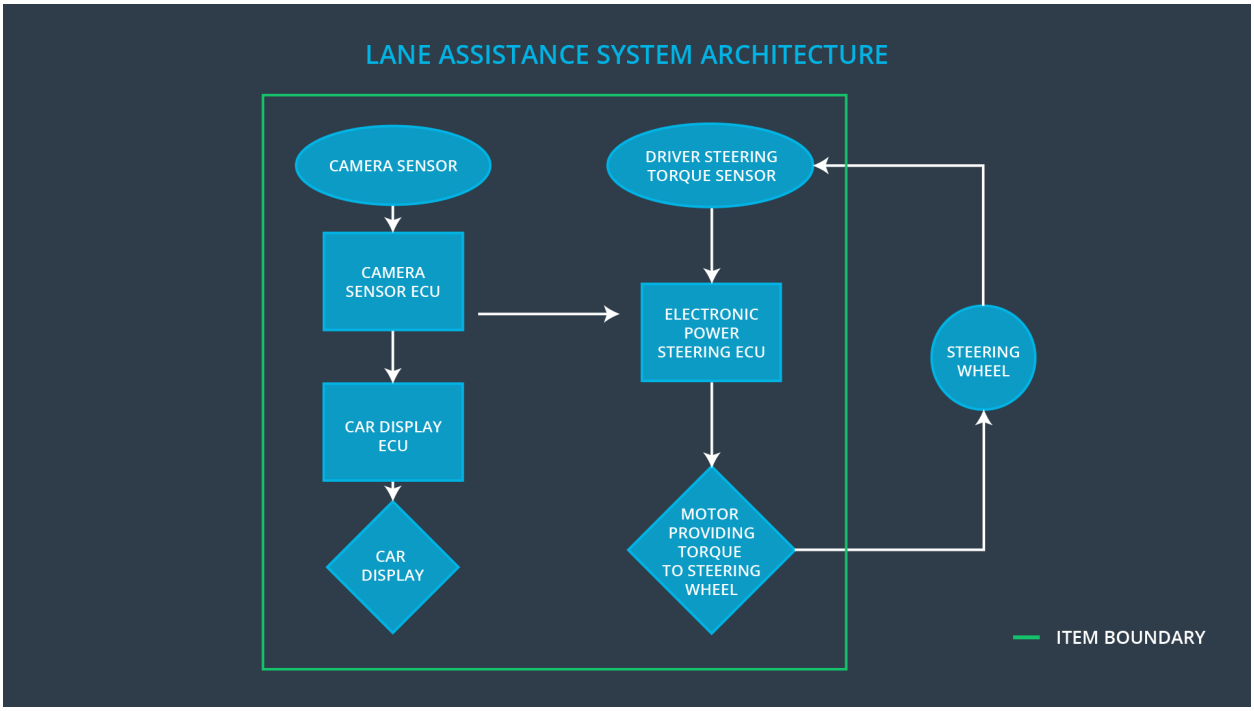
The purpose of the functional safety concept is to provide a high level overview of the system. It uses the Hazard Analysis and Risk Assessment to to define what the system should do in order to reduce risks associated for the Lane Assistance system to acceptable level. The Functional Safety Concept doesn't provide implementation details for the system. It simply provides what behavior is expected and gives steps for verifying and validating the requirements

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

| ID | Safety Goal |
|---|---|
| Safety_Goal_01 | The oscillating steering wheel torque and frequency from the Lane Departure Warning function system be limited |
| Safety_Goal_02 | The lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving |

## Preliminary Architecture



### Description of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | The camera sensor reads in images from the front of the car |
| Camera Sensor ECU | The camera sensor ECU identifies when the vehicle has departed its lane and sends the following<br>1. A steering command to the power steering ECU to bring the car back into it's lane and to virate the steering wheel to aleart the driver<br>2. A message to the Car display ECU to show a warning to the user that the car is drifting out of it's lane |
| Car Display | Screen to show warning and information messages |
| Car Display ECU | Control unit to receive messages from the Camera Sensor ECU and then control the Car Display to show the appropriate message / warning to the driver through the car display |
| Driver Steering Torque Sensor | Sensor that measures the amount and direction of torque applied by the driver to the steering wheel |
| Electronic Power Steering ECU | Control unit responsible for receiving steering command messages from the camera sensor ECU and producing appropriate motion commands to the motor |
| Motor | Applies torque 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 | 50ms | Reduce torque amplitude to 0 |
| Functional Safety Requirement 01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | C | 50ms | Reduce vibration frequency to 0 |

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 | Validate that Max_Torque_Amplitude is acceptable to drivers and will allow them keep control of the vehicle | Test system by requesting more torque than Max_Torque_Amplitude. Verify that torque does not exceed Max_Torque_Amplitude and is back down within 50ms if it does go above for whatever reason |
| Functional Safety Requirement 01-02 | Validate that Max_Torque_Frequency is acceptable to drivers and will allow them to keep control of the vehicle | Test system by requesting more torque frequency than Max_Torque_Frequency. Verify that frequency does not exceed Max_Torque_Frequency and is back down within 50ms if it does go above for whatever reason |

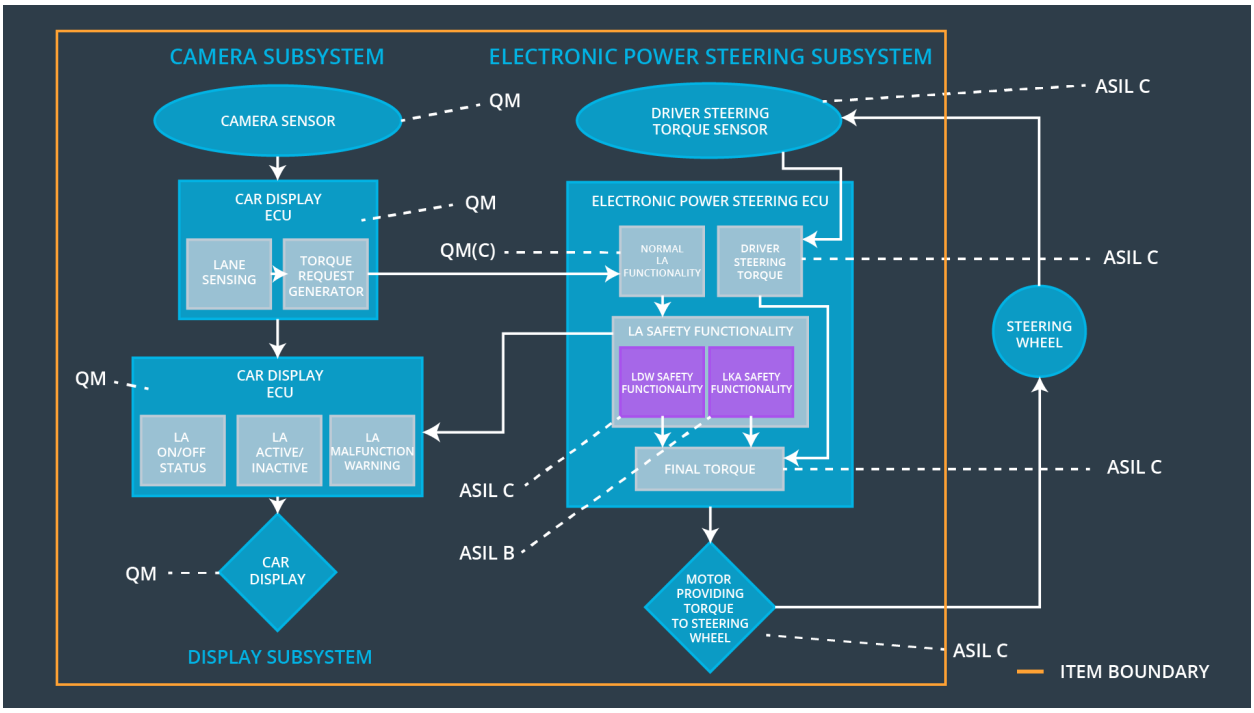
Lane Keeping Assistance (LKA) Requirements:

| 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 torque reduced to 0 |

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 | Validate that Max_Duration is sufficiently short to prevent the user from getting complacent and is long enough that it is not unnecessarily annoying | Verify that the Lane Keeping Assistance function activation time does not exceed Max_Duration. If it does, the system should shutdown within 500ms of 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 Lane Departure Warning function | Malfunction_01<br>Malfunction_02 | Yes | Warning light on dashboard |
| WDC-02 | Turn off Lane Keeping Assistance function | Malfunction_03 | Yes | Warning light on dashboard |