Elektrobit

UDACITY

# Functional Safety Concept Lane Assistance

**Document Version: 1.0**

**Released on 2018-09-10**

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 09/10/2018 | 1.0 | Vianney Monestel | First release |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Functional Safety Concept

The functional safety concept looks at the general functionality of the item. The idea is to define the system high level requirements related to safety. The functional safety concept does not go into technical details, it looks at the item at a higher level view. These functional safety requirements are derived from the Safety Goals defined in the Hazard Analysis and Risk Assessment process.

When the safety requirements are defined, they are allocated to the parts of the system diagram; that means definition of which part of the system architecture will implement each requirement. The system architecture will be refine to handle the new requirements. Finally, there is a verification and validation process where the system is tested to prove it meets the safety 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 torque from the Lane Departure Warning function shall be limited. |
| Safety_Goal_02 | The Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving. |

## Preliminary Architecture

The next figure shows the initial architecture for the lane assistance system:

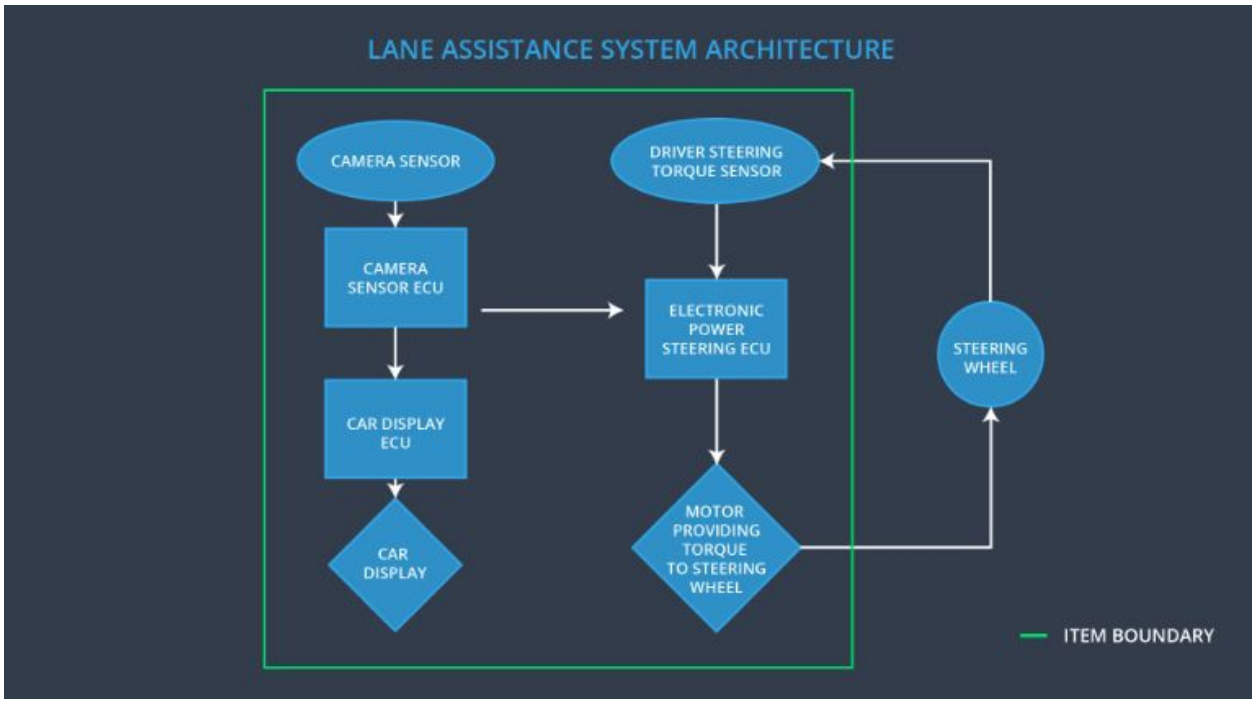


Figure 1. Initial Lane Assistance System Architecture

## Description of architecture elements:

| Element | Description |
|---|---|
| Camera Sensor | Capture lane images and provide them to the Camera Sensor ECU. |
| Camera Sensor ECU | Analyze lane images and car's position respect to its lane. It also sends a signal to the Electronic Power Steering ECU to request torque or vibration in the wheel. |
| Car Display | Show warnings on the car's dashboard. |
| Car Display ECU | Generate the dashboard warnings to the driver to show the Lane Keeping Assistance and Lane Departure status. |

| | |
|---|---|
| Driver Steering Torque Sensor | Determine the torque amount applied to the wheel by the driver. |
| Electronic Power Steering ECU | Determine if extra steering torque is needed to help the driver move back towards the center of the lane. |
| Motor | Receive the final torque amount and applies it 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 | Vibration amplitude is below Max_Torque_Amplitude value |
| 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 | Vibration frequency is below Max_Torque_Frequency value |

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

| ID | Validation Acceptance Criteria and Method | Verification Acceptance Criteria and Method |
|---|---|---|
| Functional | Test how drivers react to different | Verify that the torque amplitude |

| | | |
|---|---|---|
| Safety Requirement 01-01 | torque amplitudes and validate that the chosen amplitude is high enough to be detected. | never exceeds Max_Torque_Amplitude value. |
| Functional Safety Requirement 01-02 | Test how drivers react to different torque frequencies and validate that the chosen value is the right one so the driver does not lose control of the wheel. | Verify that the torque frequency never exceeds Max_Torque_Frequency value. |

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 | System is 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 | Validate that the max_duration chosen really did dissuade drivers from taking their hands off the wheel | Verify that the system turns off the LKA when Max_Duration time is exceeded. |

## Refinement of the System Architecture

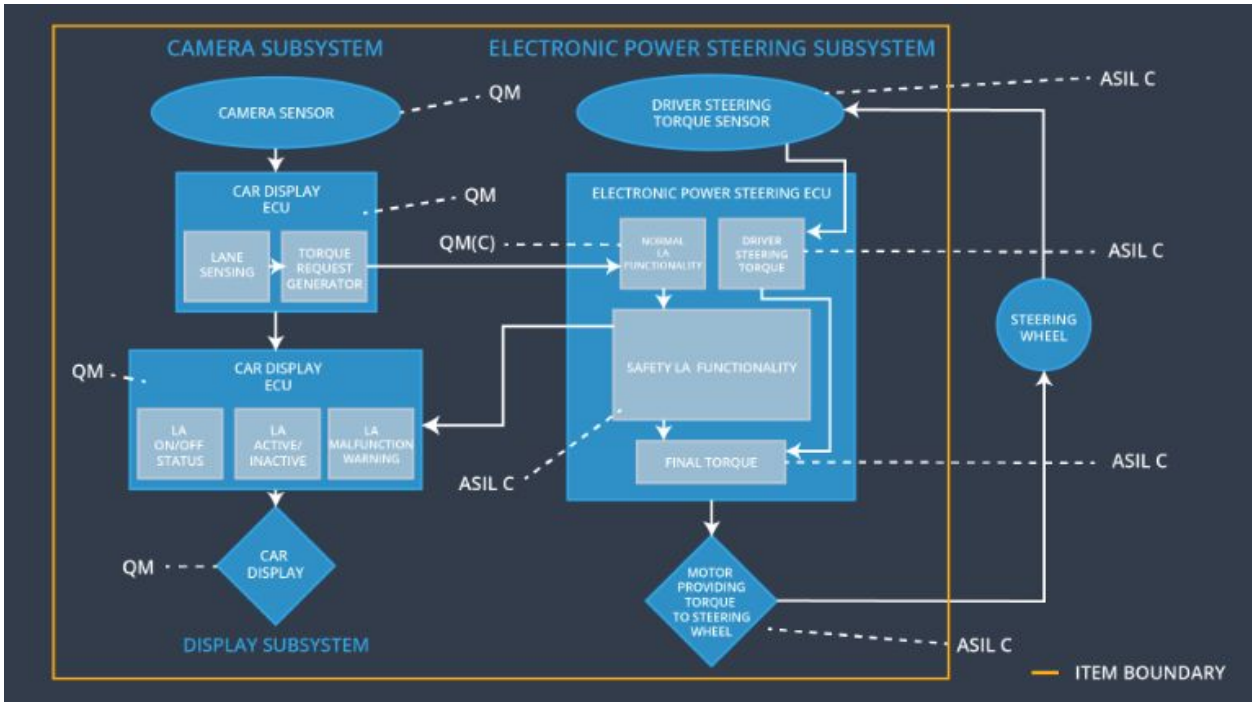


Figure 2. Final System Architecture with ASIL labels

## 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 Requiremen | The lane keeping item shall ensure that the lane departure oscillating torque frequency is | **X** | | |

| | | | | |
|---|---|---|---|---|
| t<br>01-02 | below<br>Max_Torque_Frequency | | | |
| Functional Safety Requirement<br>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 system | Malfunction_01<br>Malfunction_02 | Yes | Lane Departure Malfunction warning displayed to the driver. |
| WDC-02 | Turn off the system | Malfunction_03 | Yes | Lane Keeping Assistance warning displayed to the driver. |