Elektrobit

UDACITY

# Functional Safety Concept Lane Assistance

## Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 28th May, 2018 | 1.0 | Anant Yash Pande | Initial document |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

# Table of Contents



# Purpose of the Functional Safety Concept

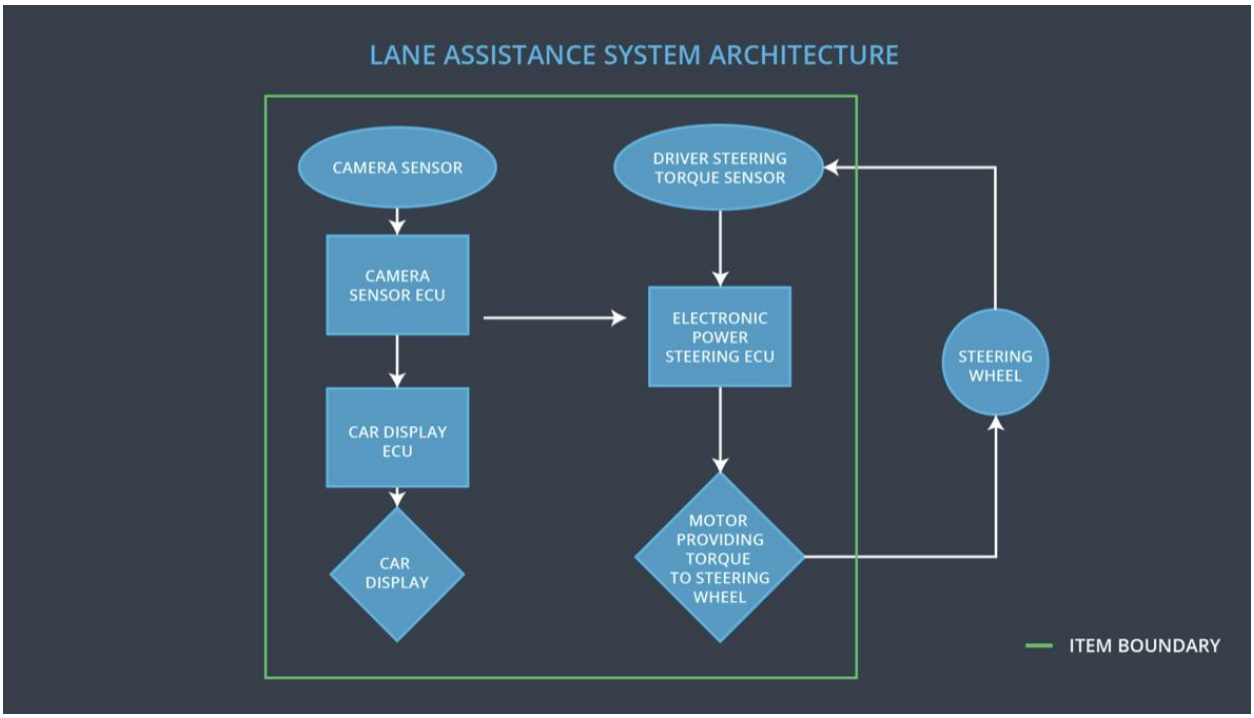
The document should cover the general functionality of the object, without going into the technical detail. This document also identifies safety requirements and then assigns these requirements to different parts of the item architecture. Functional safety requirements also have attributes that are specified in the functional safety concept. To prove that a system actually meets the requirements, they must be verified and validated.

# 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 of the lane departure warning must be limited. |
| Safety_Goal_02 | The lane departure warning function must be limited based on active time and after that the control should be returned to the driver. |

## Preliminary Architecture




### Description of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | Captures images and feeds them to the Camera Sensor ECU. |

| | |
|---|---|
| Camera Sensor ECU | Detects lane lines and positions of the car with respect to lane |
| Car Display | Provides feedback to the driver, displays warnings and the Lane Departure Assistance status. |
| Car Display ECU | Controls the display unit of car and based on inputs from other units. |
| Driver Steering Torque Sensor | Measures the torque applied to the steering wheel. |
| Electronic Power Steering ECU | Based on inputs from Driver Steering Torque Sensor and camera ECU it calculates the amount of torque to be applied on steering wheel. |
| Motor | Applies the torque indicated 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 system applies an oscillating torque with very high amplitude |
| Malfunction_02 | Lane Departure Warning (LDW) function shall apply | MORE | The lane departure warning function |

| | | | |
|---|---|---|---|
| | an oscillating steering torque to provide the driver a haptic feedback | | 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 | 50 ms | Set Vibration to zero when fault detected |
| 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 | Set Vibration to zero when fault detected |

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 | The Max_Torque_Amplitude chosen is high enough to warn driver while low enough not to cause loss of control | Check whether systems are turned off when Max_Torque_Frequency greater than the safe limit. |
| Functional Safety | The Max_Torque_Amplitude chosen is | Check whether systems are turned off when Max_Torque_Frequency is |

| | | |
|---|---|---|
| Requirement 01-02 | high enough to warn the driver and not cause the loss of control. | greater than the safe limit. |

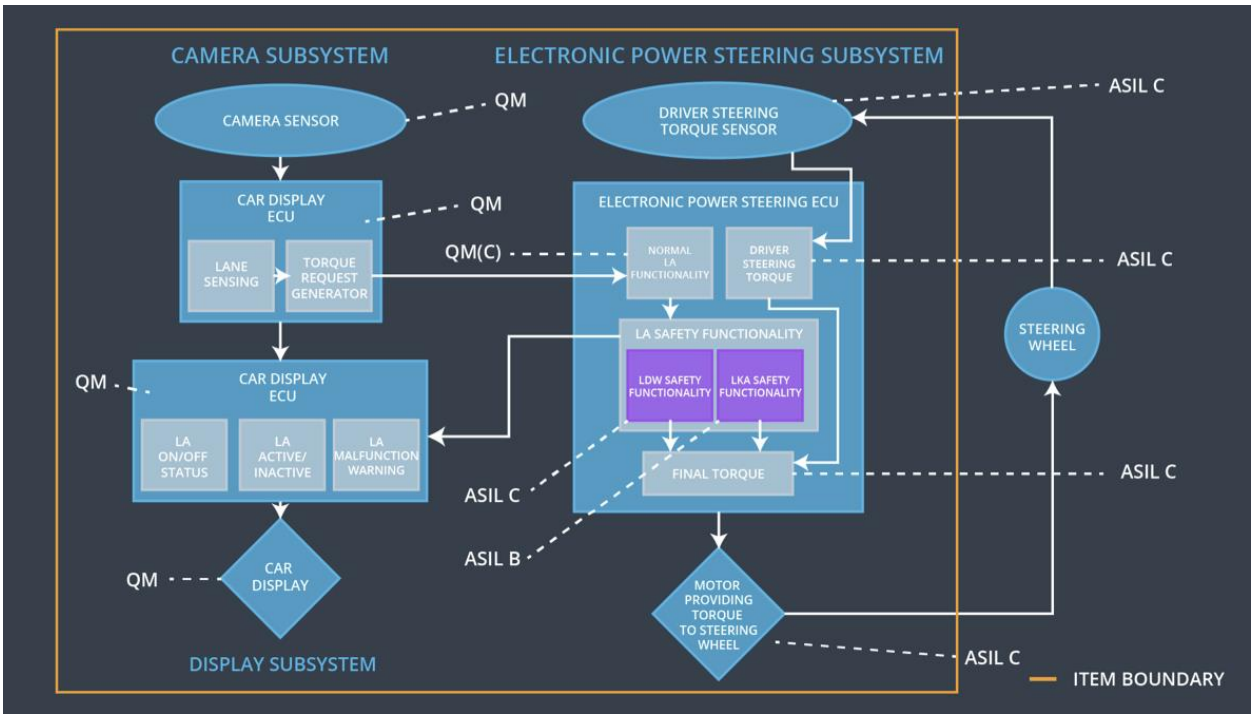
Lane Keeping Assistance (LKA) Requirements:

| 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 not applied after the Max_Duration | B | 500 ms | Reduce the torque by lane keeping system to zero when fault is detected |

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 is enough to discourage the drivers from leaving the steering wheel | Verify that the system really does turn off if the lane keeping assistance is active for more than the max duration. |

## Refinement of the System Architecture




## Allocation of Functional Safety Requirements to Architecture Elements

**[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]**

| 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 | Responsible | Not responsible | Not responsible |
| Functional Safety Requirement 01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | Responsible | Not responsible | Not responsible |
| Functional Safety | The electronic power steering ECU shall ensure that the lane | Responsible | Not responsibl | Not responsible |

| | | | | |
|---|---|---|---|---|
| Requirement 02-01 | keeping assistance torque is not applied more than Max_Duration | | e | |

## Warning and Degradation Concept

**[Instructions: Fill in the warning and degradation concept.]**

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | Lane Departure warning functionality is set to zero | Malfunction_01<br>Malfunction_02 | Yes | Malfunction warning on with Lane Departure warning indicator signal |
| WDC-02 | Lane keeping assistance functionality is set to zero | Malfunction_03 | Yes | Malfunction warning on with Lane keeping assistance indicator signal |