Elektrobit

UDACITY

# Functional Safety Concept Lane Assistance

**Document Version:** [Version]

**Template Version 1.0, Released on 2017-06-21**

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 10/15/2018 | 1.0 | Yan Cui | Initial draft |
| 10/31/2018 | 1.1 | Yan Cui | Revision for submission |
| | | | |
| | | | |
| | | | |

# Table of Contents



# Purpose of the Functional Safety Concept

**[Instructions: Answer what is the purpose of a functional safety concept?]**

In the Functional Safety Concept document, the system high level requirements are identified. These requirements are allocated to the relevant parts of the item architecture. Technical safety

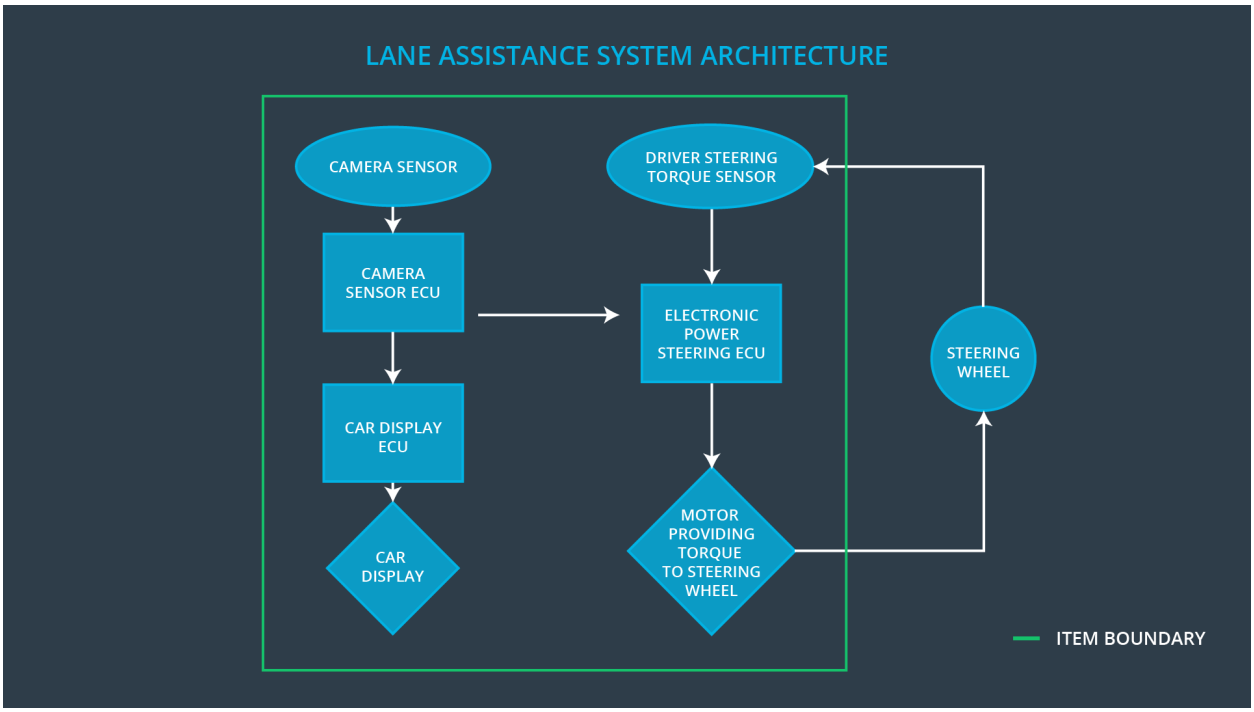
requirements will be then derived from those safety concepts. This document also includes verification and validation, which is how to prove that a system actually meets requirements.

# Inputs to the Functional Safety Concept

## Safety goals from the Hazard Analysis and Risk Assessment

| ID | Safety Goal |
|---|---|
| Safety_Goal_01 | The oscillating torque to the steering wheel from the lane departure warning function shall be limited. |
| Safety_Goal_02 | The LKA function should be time limited. Corresponding on/off should be sent to driver. |
| Safety_Goal_03 | The LDW function should be deactivated when camera is not working. |
| Safety_Goal_04 | The LKA function should be deactivated when camera is not working. |

## Preliminary Architecture



### Description of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | The Camera Sensor reads in images from the road. |
| Camera Sensor ECU | The Camera Sensor ECU identifies when the vehicle has accidentally departed its lane, and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU. |
| Car Display | The Car Display displays warning messages and the lane departure assistance status to the driver. |
| Car Display ECU | The Car Display ECU receives messages from the Camera Sensor ECU and drives the Car Display component to show message. |
| Driver Steering Torque Sensor | The Driver Steering Torque Sensor measures the torque applied on steering wheel and output messages to the Electronic Power Steering ECU. |
| Electronic Power Steering ECU | The Electronic Power Steering ECU receives messages from both the Driver Steering Torque Sensor and the Camera Sensor ECU, and also sends corresponding torque messages to the Motor. |
| Motor | The Motor receives messgae from the Electronic Power Steering ECU, and 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 | Lane Departure Warning (LDW) function applies oscillating torque with very high torque amplitude beyond limit. |
| Malfunction_02 | Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback | MORE | Lane Departure Warning (LDW) function applies an oscillating torque with very high torque frequence beyond 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 (LKA) function is not limited in use, and kept on which could lead driver misuse the autonomous driving mode. |
| Malfunction_04 | Lane Departure Warning (LDW) function shall be deactivated the time when camera sensor stops working | WRONG | Lane Departure Warning (LDW) acts randomly after camera stops working. |
| Malfunction_05 | Lane Keeping Assistance (LKA) function shall be deactivated the time when camera sensor stops working | WRONG | Lane Keeping Assistance (LKA) function acts randomly after camera stops working. |

# Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

| ID | Functional Safety Requirement | AS | Fault Tolerant | Safe State |
|---|---|---|---|---|

| | | I L | Time Interval | |
|---|---|---|---|---|
| Functional Safety Requirement 01-01 | Lane Departure Warning (LDW) function needs to ensure the oscillating torque amplitude is always below Max_Torque_Amplitude. | C | 50ms | Oscillating torque amplitude below Max_Torque_Amplitude |
| Functional Safety Requirement 01-02 | Lane Departure Warning (LDW) function needs to ensure the oscillating torque frequency is always below Max_Torque_Frequency. | C | 50ms | Oscillating torque frequency below Max_Torque_Frequency |
| Functional Safety Requirement 01-03 | Lane Departure Warning (LDW) function shall be deactivated the time when camera sensor stops working | C | 10ms | LDW is deactivated |

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 the chosen value of Max_Torque_Amplitude is within the resonable range, not making too much oscillation to driver, yet not too small to be un-detectable. | Verify that if the oscillation torque is above Max_Torque_Amplitude, the system turns off. |
| Functional Safety Requirement 01-02 | Validate the chosen value of Max_Torque_Frequency is within the resonable range, not making too much oscillation to driver. | Verify that if the oscillation torque is above Max_Torque_Frequency, the system turns off. |
| Functional Safety Requirement 01-03 | Validate the LDW function turns off when received camera error message. | Verify the LDW function is always off when camera sensor stops working. |

Lane Keeping Assistance (LKA) Requirements:

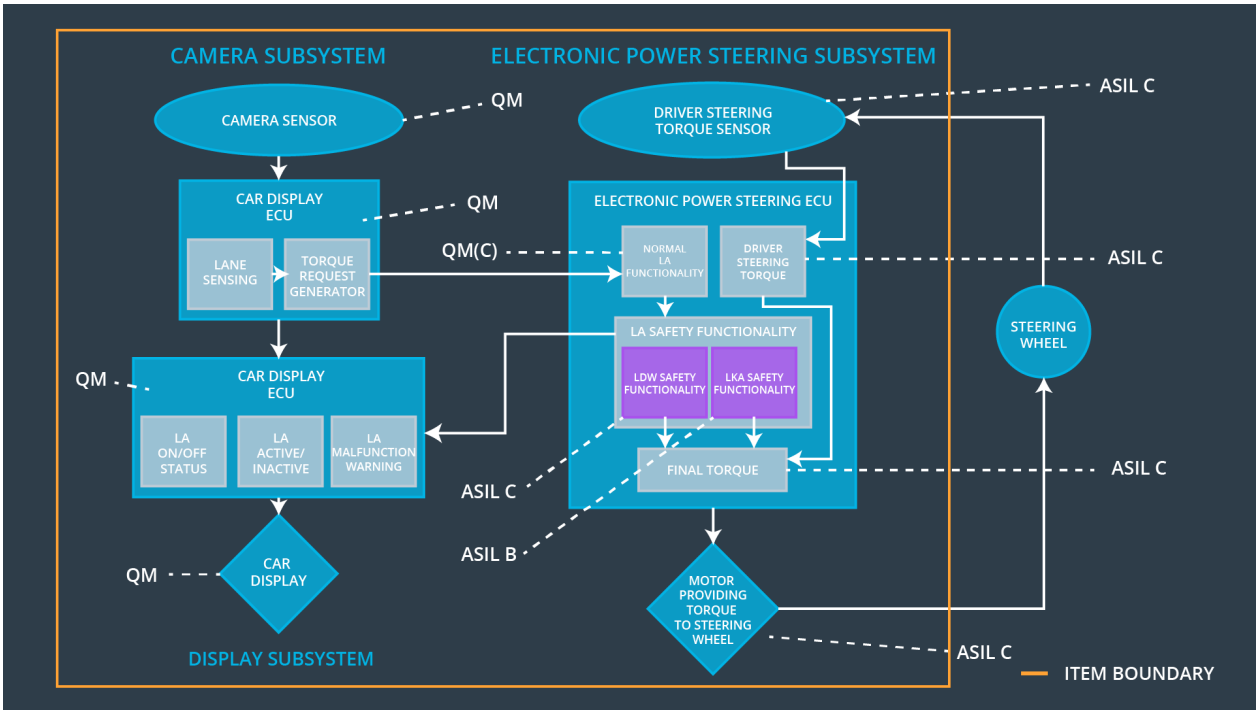
| ID | Functional Safety Requirement | ASIL | Fault Tolerant Time Interval | Safe State |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Functional Safety Requirement 02-01 | The electronic power steering ECU needs to ensure that Lane Keeping Assistance torque is applied only Max_Duration | B | 500ms | Lane Keeping Assistance torque is zero |
| Functional Safety Requirement 02-02 | The Lane Keeping Assistance (LKA) shall be deactivated the time when camera sensor stops working | D | 10ms | Function is deactivated |

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 the Max_Duration chosen not to allow use self-driving mode | Verify the system deactivates if LKA torque application exceeds Max_Duration |
| Functional Safety Requirement 02-02 | Validate the LKA function turns off when received camera error message. | Verify the LKA function is deactivated when camera sensor stops working. |

## 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 | Lane Departure Warning (LDW) function needs to ensure the oscillating torque amplitude is always below Max_Torque_Amplitude. | **X** | | |
| Functional Safety Requirement 01-02 | Lane Departure Warning (LDW) function needs to ensure the oscillating torque frequency is always below Max_Torque_Frequency. | **X** | | |
| Functional Safety Requirement | Lane Departure Warning (LDW) function shall be deactivated the time when camera sensor stops | **X** | | |

| | | | | |
|---|---|---|---|---|
| 01-03 | working | | | |
| Functional Safety Requirement 02-01 | The electronic power steering ECU needs to ensure that Lane Keeping Assistance torque is applied only Max_Duration | **X** | | |
| Functional Safety Requirement 02-02 | The Lane Keeping Assistance (LKA) shall be deactivated the time when camera sensor stops working | **X** | | |

## Warning and Degradation Concept

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | Turn off Lane Departure Warning (LDW) function | Malfunction_01, Malfunction_02, Malfunction_04 | Yes | Lane Departure Warning (LDW) malfunction warning on Car Display |
| WDC-02 | Turn off Lane Keeping Assistance (LKA) function | Malfunction_03, Malfunction_05 | Yes | Lane Keeping Assistance (LKA) malfunction warning on Car Display |