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 |
|---|---|---|---|
| 1/6/2018 | 1.0 | Pratul Singh | Initial Attempt |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents



# Purpose of the Functional Safety Concept

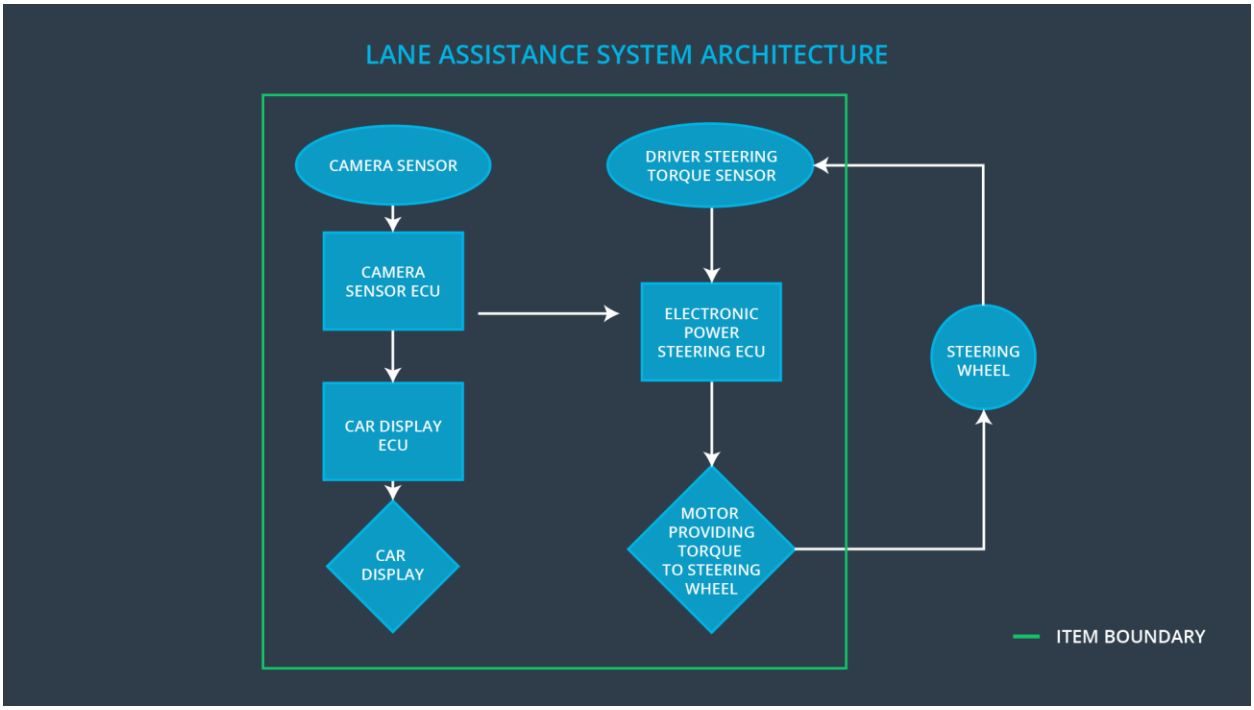
The purpose of the functional safety concept is to identify new system level requirements and allocate these requirements to high level system diagrams for the lane assistance functional safety project as pertain to the potential malfunctions of the electrical and electronic systems as defined by ISO 26262 standard, tailored.

# 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 system 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 | Sensor responsible for capturing vehicle driving condition including detectable lane lines |
| Camera Sensor ECU | Determine if the car is leaving the lane and if so, send a vibrational torque request to the power steering ECU |
| Car Display | Visual display responsible to displaying warning of lane departures and LKA and LDW activation and deactivations. |
| Car Display ECU | Receives signals from the camera ECU if either of the functions have been activated |
| Driver Steering Torque Sensor | Senses how much torque is already being applied to the steering wheel. |
| Electronic Power Steering ECU | Receives the vibrational torque request from the camera ECU. Computes the residual torque needed to be applied after considering the input from the torque sensor. Sends the torque output request to the motor |
| Motor | Actuator responsible for applying requested torque to the steering column by the Electronic Power Steering ECU for either the LKA or the LDW functions. |

# 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 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 torque amplitude to zero |

| | | | | |
|---|---|---|---|---|
| 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 torque frequency to zero. |

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 MAX_Torque_Amplitude chosen is high enough to be detected by driver while low enough not to cause loss of steering. | Verify that the system does turn off if the lane departure warning ever exceeded MAX_Torque_Amplitude |
| Functional Safety Requirement 01-02 | Validate MAX_Torque_Fequency chosen is high enough to be detected by driver while low enough not to cause loss of steering. | Verify that the system does turn off if the lane departure warning ever exceeded MAX_Torque_Fequency |

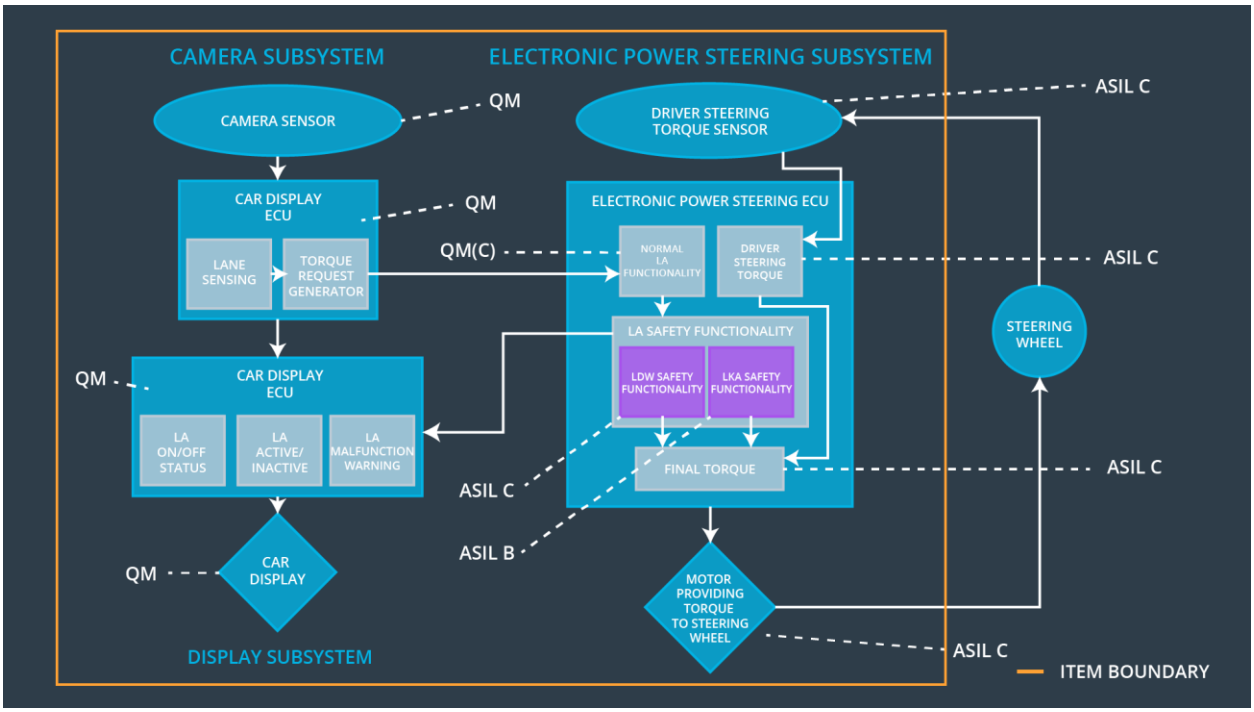
Lane Keeping Assistance (LKA) Requirements:

| 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 | 500 ms | Lane Keeping assistance system is not activated |

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 did dissuade drivers from taking their hands off the wheel. | The system does turn off if the lane keeping assistance every exceeded 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 electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude | YES | NO | NO |
| Functional Safety Requirement 01-02 | The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency | YES | NO | NO |

| | | | | |
|---|---|---|---|---|
| Functional Safety Requirement 02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration | YES | NO | NO |

## Warning and Degradation Concept

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | Turn off functionality | The malfunction of the steering wheel vibrating too much | Yes | Warning light on the dashboard |
| WDC-02 | Turn off functionality | The malfunction of the lane keeping assistance function being applied for too long | Yes | Warning light on the dashboard |