# Functional Safety Concept Lane Assistance

**Document Version:** [Version]

Template Version 1.0, Released on 2017-06-21

# Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

| Date | Version | Editor | Description |
|---|---|---|---|
| 11/01/2018 | 1.0 | BM | First version of the document |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Purpose of the Functional Safety Concept

The functional safety concept is the document that contains the high level view of the functional safety requirements for the project. The functional safety concept does not go deep into describing the technical details of the functional safety requirements, but it serves as the starting point to the document called technical safety concept, which describes the technical details of the functional 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. |
| Safety_Goal_03 | The Lane Departure Warning function shall be deactivated in the absence of incoming requests from the camera subsystem. |
| Safety_Goal_04 | The Lane Keeping Assistance function shall be deactivated in the absence of incoming requests from the camera subsystem. |

## Preliminary Architecture

The following figure shows the preliminary architecture of the Lane Assistance System.

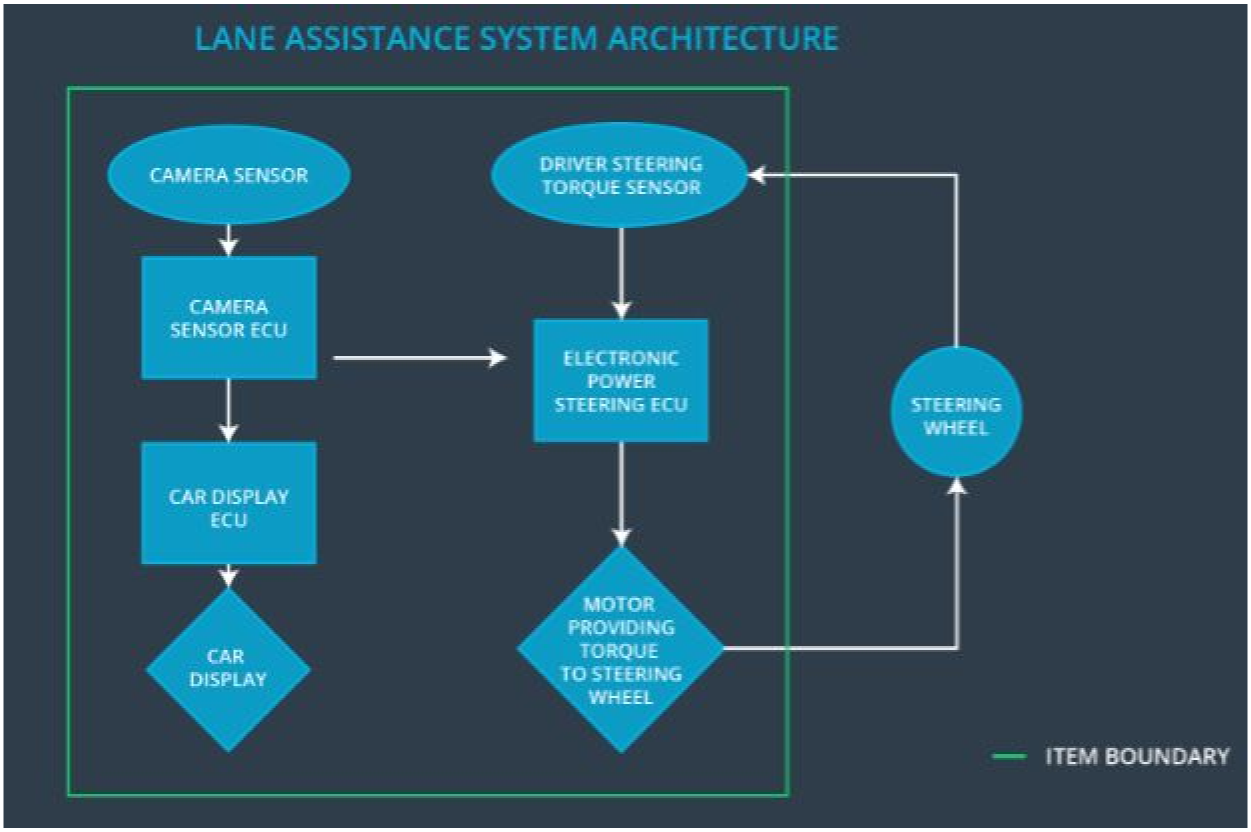
LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

Figure 1. Preliminary Lane Assistance System architecture

## Description of architecture elements

| Element | Description |
|---|---|
| Camera Sensor | The front facing camera that captures the road ahead and provides the images to the camera sensor ECU |
| Camera Sensor ECU | Analyzes the images from the camera sensor, calculates the position of the vehicle with respect to the center of the ego lane, and sends the appropriate signals to the car display subsystem and the electronic power steering subsystem. |
| Car Display | Provides the information to the driver about the current status of the Lane Assistance System (whether it is turned on and if it is currently |

| | |
|---|---|
| | performing any action) |
| Car Display ECU | Controls the car display and ensures its operation |
| Driver Steering Torque Sensor | Senses the torque exerted on the steering wheel by the driver |
| Electronic Power Steering ECU | Takes as inputs the signals from the driver steering torque sensor and the camera subsystem, and controls the motor steering the wheel, to achieve the correct final steering torque |
| Motor | Steers the steering wheel with the amount of torque calculated by the electronic power steering ECU |

# 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

**[Instructions: Fill in the functional safety analysis table below.]**

| **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 | LDW 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 | LDW 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 | LKA is not limited in time duration which lead to misuse as an autonomous driving function. |
| Malfunction_04 | Lane Departure Warning (LDW) function shall be deactivated in the absence of incoming requests from the camera subsystem. | WRONG | LDW acts randomly when the camera subsystem is not sending requests. |
| Malfunction_05 | Lane Keeping Assistance (LKA) function shall be deactivated in the absence of incoming requests from the camera subsystem. | WRONG | LKA acts randomly when the camera subsystem is not sending requests. |

## 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 Departure Warning function shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude. | C | 50 ms | Function is deactivated. |
| Functional Safety Requirement 01-02 | The Lane Departure Warning function shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency. | C | 50 ms | Function is deactivated. |
| Functional Safety Requirement 01-03 | The Lane Departure Warning function shall be deactivated in the absence of incoming requests from the camera subsystem. | C | 50 ms | Function 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 | Test different values of Max_Torque_Amplitude to ensure that the proper value is chosen for driver’s comfort while still preserving meaningful functionality. | Ensure that the function is deactivated if the amplitude is higher than Max_Torque_Amplitude for the given fault tolerant time interval. |

| | | |
|---|---|---|
| Functional Safety Requirement 01-02 | Test different values of Max_Torque_Frequency to ensure that the proper value is chosen for driver’s comfort while still preserving meaningful functionality. | Ensure that the function is deactivated if the amplitude is higher than Max_Torque_Frequency for the given fault tolerant time interval. |
| Functional Safety Requirement 01-03 | Validate that LDW performs no action when the camera subsystem is not sending any requests. | Ensure that LDW performs no action when the camera subsystem is not sending any requests for the given fault tolerant time interval. |

**[Instructions: Fill in the functional safety requirements for the lane keeping assistance]**

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 torque for the Lane Keeping Assistance function is applied for no longer than Max_Duration time interval. | B | 500 ms | Function is deactivated. |
| Functional Safety Requirement 02-02 | The Lane Keeping Assistance function shall be deactivated in the absence of incoming requests from the camera subsystem | C | 50 ms | 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 that the proper value is chosen for Max_Duration that prevents the drivers from using the LKA function as the self-driving capability of the vehicle. | Verify that LKA deactivates if the duration of the applied torque exceeds Max_Duration. |
| Functional Safety Requirement 02-02 | Validate that LKA performs no action when the camera subsystem is not sending any requests. | Ensure that LKA performs no action when the camera subsystem is not sending any requests for the given fault tolerant time interval. |

## Refinement of the System Architecture

The refined system architecture is shown in Figure 2.

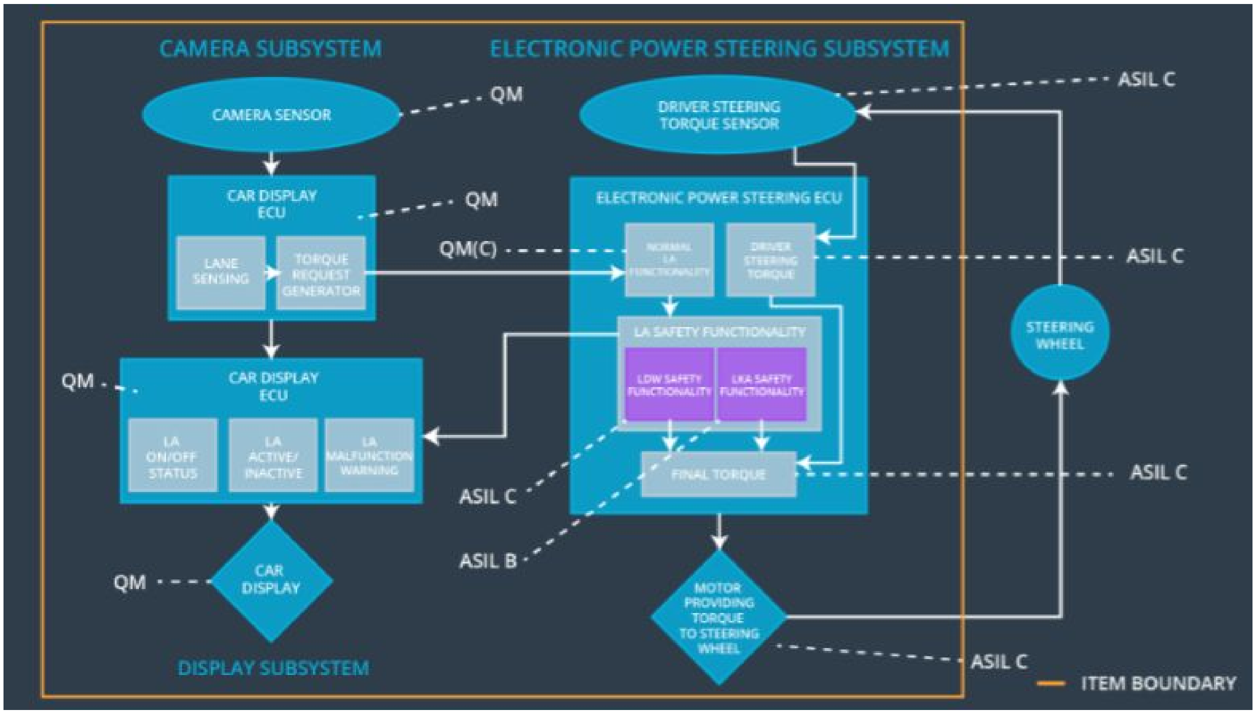

Figure 2. Refinement of the system architecture

## 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 Departure Warning function shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude. | **X** | | |
| Functional Safety Requirement 01-02 | Test different values of Max_Torque_Frequency to ensure that the proper value is chosen for driver's comfort while still preserving meaningful functionality. | **X** | | |
| Functional Safety Requirement 01-03 | Validate that LDW performs no action when the camera subsystem is not sending any requests. | **X** | | |
| Functional Safety Requirement 02-01 | The electronic power steering ECU shall ensure that the torque for the Lane Keeping Assistance function is applied for no longer than Max_Duration time interval. | **X** | | |
| Functional Safety Requirement 02-02 | The Lane Keeping Assistance function shall be deactivated in the absence of incoming requests from the camera subsystem | **X** | | |

## Warning and Degradation Concept

| ID | Degradation Mode | Trigger for Degradation Mode | Safe State invoked? | Driver Warning |
|---|---|---|---|---|
| WDC-01 | Turn off Lane Assistance System | Malfunction_01 | Yes | Lane Assistance System malfunction warning on car display |
| WDC-02 | Turn off Lane Assistance System | Malfunction_02 | Yes | Lane Assistance System malfunction warning on car display |
| WDC-03 | Turn off Lane Assistance System | Malfunction_03 | Yes | Lane Assistance System malfunction warning on car display |
| WDC-04 | Turn off Lane Assistance System | Malfunction_04 | Yes | Lane Assistance System malfunction warning on car display |
| WDC-05 | Turn off Lane Assistance System | Malfunction_05 | Yes | Lane Assistance System malfunction warning on car display |