



Elektrobit



UDACITY

# 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
03.06.2018	1.1	Ankith Manjunath	Functional safety concept first version

# Table of Contents

[Document history](#)

[Table of Contents](#)

[Purpose of the Functional Safety Concept](#)

[Inputs to the Functional Safety Analysis](#)

[Safety goals from the Hazard Analysis and Risk Assessment](#)

[Preliminary Architecture](#)

[Description of architecture elements](#)

[Functional Safety Concept](#)

[Functional Safety Analysis](#)

[Functional Safety Requirements](#)

[Refinement of the System Architecture](#)

[Allocation of Functional Safety Requirements to Architecture Elements](#)

[Warning and Degradation Concept](#)

## Purpose of the Functional Safety Concept

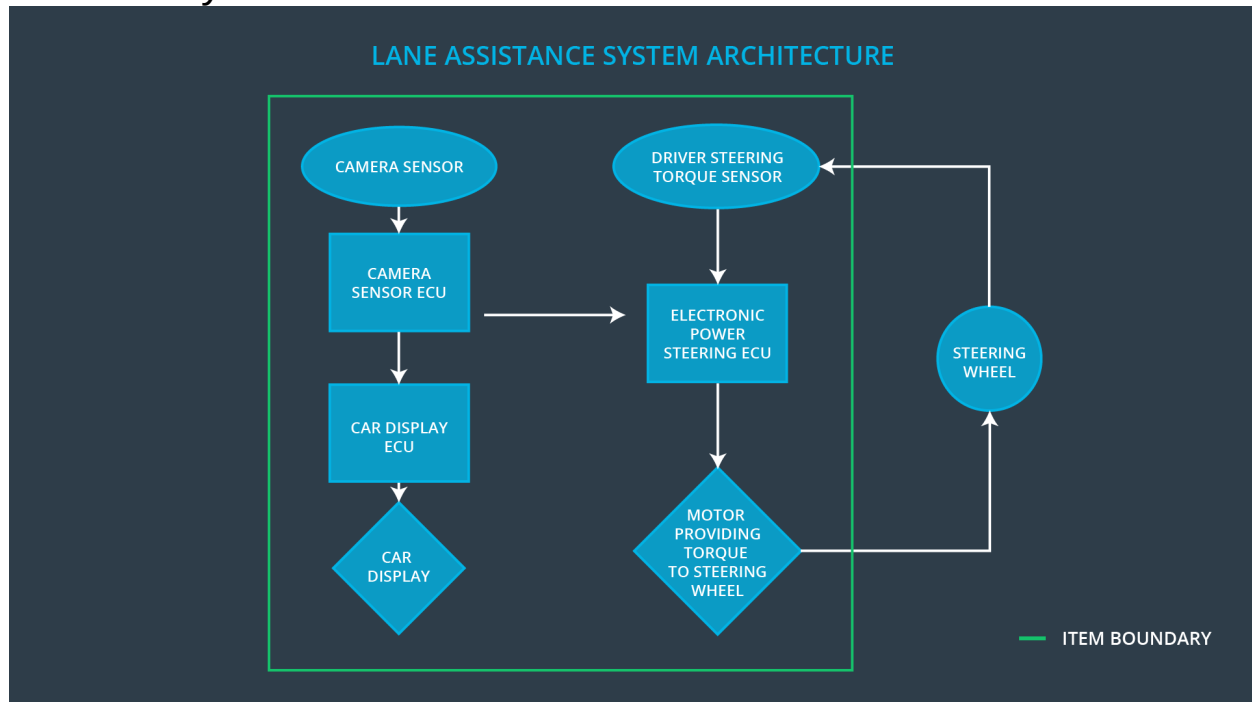
The main higher view of functional safety concept for a system under test is to make the system functionally safe. Functionally safe system has to reduce the impact of occurring hazardous situations.

## Inputs to the Functional Safety Concept

### Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The lane departure warning subsystem shall apply an oscillating torque less than the limit
Safety_Goal_02	The lane keeping assistance shall be time limited and shall apply steering torque for a limited period of time

## Preliminary Architecture



## Description of architecture elements

[

Element	Description
Camera Sensor	Provide video feed of the road in front of the vehicle
Camera Sensor ECU	Detect lane markings from the video feed. Detect the position of the vehicle from the center of the lane.
Car Display	Display to the driver if functionality is on/off. Display the driver for a gradual degradation
Car Display ECU	Receive data about function on/off and also for function gradual degradation
Driver Steering Torque Sensor	Sense the steering wheel torque from the driver
Electronic Power Steering ECU	Determine the amount of steering torque needed for the functionality and normal operation mode
Motor	Provide the required torque from the software torque input

# 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 lead to misuse as an autonomous driving function.

## Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	A S I L	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the torque amplitude by lane departure warning system is below MAX_TORQUE_AMPLITUDE	C	50ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the torque frequency by the lane departure warning is below MAX_TORQUE_FREQUENCY	C	50ms	Vibration torque amplitude below Max_Torque_Frequency.

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	Choose a suitable value for MAX_TORQUE_AMPLITUDE	Verify the FTTI and safe state degradation using the validated MAX_TORQUE_AMPLITUDE
Functional Safety Requirement 01-02	Choose a suitable value for MAX_TORQUE_FREQUENCY	Verify the FTTI and safe state degradation using the validated MAX_TORQUE_FREQUENCY

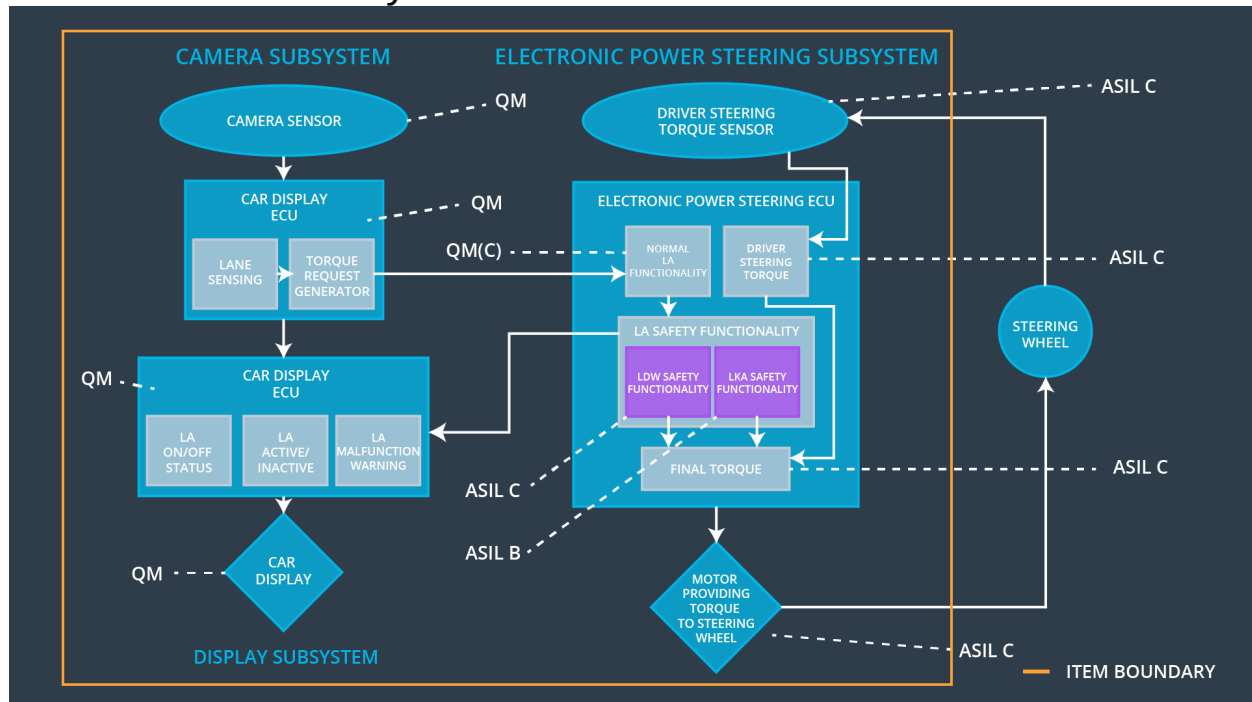
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	A S I L	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the steering torque TIME_FOR_TORQUE is applied for a limited period of time .	B	500ms	Lane Keeping Assistance torque is zero.

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 TIME_FOR_TORQUE such that the system is not misinterpreted as an autonomous function	The FTTI and safe state is verified using the validated TIME_FOR_TORQUE

## 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 keeping item shall ensure that the torque amplitude by lane departure warning system is below MAX_TORQUE_AMPLITUDE	x	-	-
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the torque frequency by the lane departure warning is below MAX_TORQUE_FREQUENCY	x	-	-
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the steering torque TIME_FOR_TORQUE is applied for a limited period of time .	x	-	-



## Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off functionality	Malfunction_01 Malfunction_02	Yes	LDW warning on the screen
WDC-02	Turn off functionality	Malfunction_03	Yes	LKA warning on the screen, Driver to take over the car