



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
5/25/2018	1.0	Kiran Acharya	FS Concept Lane Assistance – Attempt 1

## 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 functional safety concept looks at the general functionality of the item from a higher level. The goal is to identify safety requirements and then allocate those requirements to different parts of the item architecture. From the result of the functional safety concept, technical safety requirements can be derived.

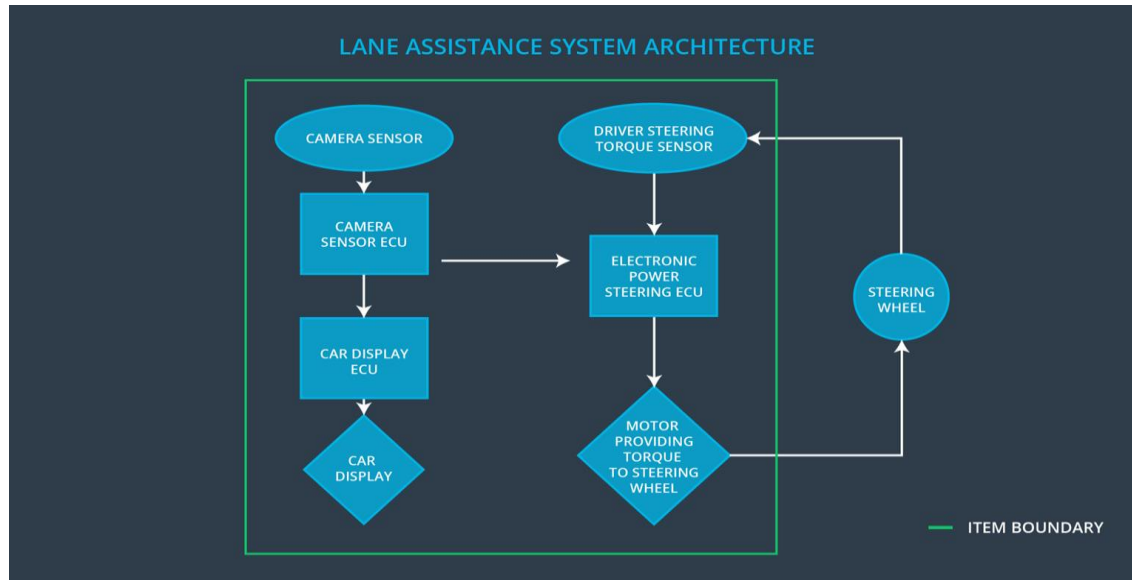
## Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the LDW function shall be limited.
Safety_Goal_02	LKA function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving.
Safety_Goal_03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.
Safety_Goal_04	The Lane Keeping Assistance function shall be deactivated when the camera sensor stop working.

# Preliminary Architecture

Following figure describes the architecture of the lane assistance item.



## Description of architecture elements

Element	Description
Camera Sensor	Provides camera images to the Camera Sensor ECU
Camera Sensor ECU	Detects lane line positions from camera images and generates a torque request to the Electronic Power Steering ECU.
Car Display	Shows warning to driver.
Car Display ECU	Generates warning signals triggered by input from Camera Sensor ECU and Electronic Power Steering ECU.
Driver Steering Torque Sensor	Delivers steering torque intensity provided by driver to Electronic Power Steering ECU.
Electronic Power Steering ECU	Processes inputs from Camera Sensor ECU, Driver Steering Torque Sensor and computes appropriate Lane Assistance functionality resulting in final torque which is transfered to the steering wheel motor.
Motor	Receives final torque calculated by Electronic Power Steering ECU and applies it to 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 function applies an oscillating torque with very high torque amplitude (above limit)
Malfunction_02	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.
Malfunction_03	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	WRONG	The Lane Departure Warning start acting randomly when the camera sensor is not working.
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	The Lane Keeping Assistance start acting randomly when the camera sensor is not working.

# 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 lane departure oscillating torque <i>amplitude</i> is below Max_Torque_Amplitude	C	50 ms	Lane Assistant functionality off
Functional Safety Requirement 01-02	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	C	10 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	Validate how drivers react to different torque amplitudes to prove that an appropriate value was chosen.	Verify that Lane Assistant functionality turns off if LKA ever exceeds Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate Lane Departure Warning is off when the camera sensor is not working.	Verify the Lane Departure Warning is never on when the camera sensor is not working.

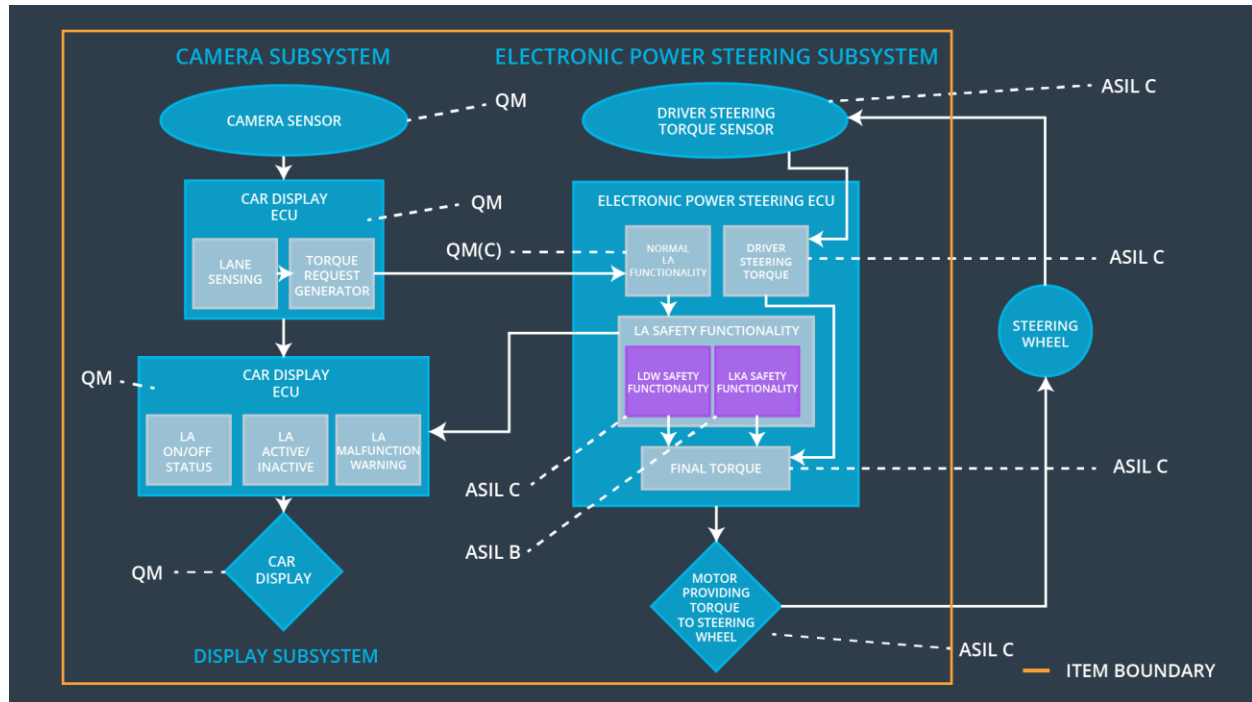
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	Lane Assistant functionality off
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working.	C	10 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	Test and validate that the Max_Duration chosen really dissuades drivers from taking their hands off the wheel.	Verify that Lane Assistant functionality turns off if LKA ever exceeds MAX_DURATION.
Functional Safety Requirement 02-02	Validate the Lane Keeping assistance shall be deactivated when the camera sensor stop working.	Verify the system does deactivate the Lane Keeping Assistance if the camera sensor is not 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	The electronic power steering ECU shall ensure that the lane departure oscillating torque <i>amplitude</i> is below Max_Torque_Amplitude	x		
Functional Safety Requirement 01-02	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	x		



Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	X		
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working.	X		

## Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Assistant functionality	Malfunction_01	Yes	Lane Assistant Malfunction Warning on Car Display
WDC-02	Turn off Lane Assistant functionality	Malfunction_02	Yes	Lane Assistant Malfunction Warning on Car Display
WDC-03	Turn off Lane Departure Warning functionality	Malfunction_03	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-04	Turn off Lane Keeping Assistance functionality	Malfunction_04	Yes	Lane Keeping Assistance Malfunction Warning on Car Display