Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 2.0
Released on 2018-06-15

Document history

Date	Version	Editor	Description
08-Jun-2018	0.1	Nikhil Patel	Initial Draft
13-Jun-2018	1.0	Nikhil Patel	Added details on "Hazard Analysis And Risk Assessment" document
15-Jun-2018	2.0	Nikhil Patel	Feedback from Udacity Reviewer

Table of Contents

Contents

Purpose of the Functional Safety Concept

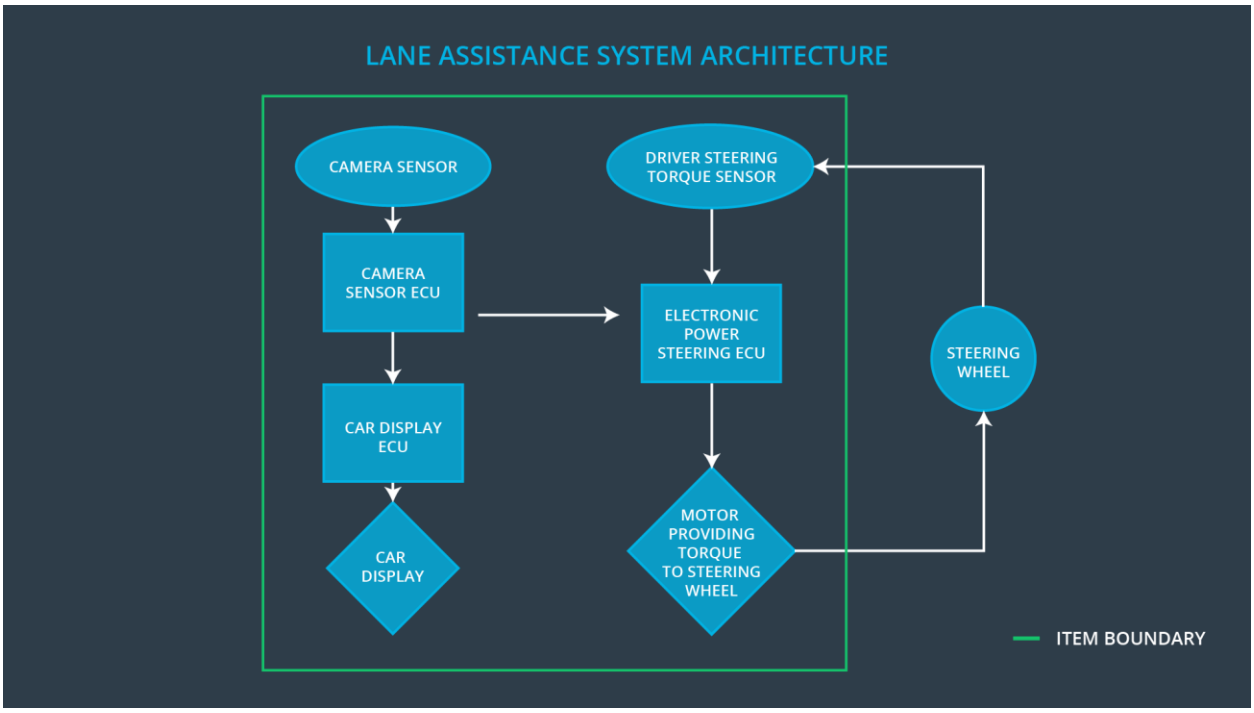
The purpose of Functional Safety Concept document is to identify system high level requirements and allocate them to different parts of the item architecture without going into technical detail. Finally, to prove that a system actually meets requirements, they have to be verified and validated. The information in the functional safety analysis comes from the hazard analysis and risk assessment. The guide words help to analyze functions and malfunctions methodically. The malfunctions are then converted into functional safety requirements

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	Steering wheel oscillations should be limited to reasonable levels
Safety_Goal_02	The Lane Keeping Assistance function must engage for certain number of times in given duration and thereafter alert the driver and disengage to prevent misuse
Safety_Goal_03	The Lane departure warning system should be deactivated when driving on roads with faded or missing lane markings
Safety_Goal_04	The amount of torque applied by Lane Keeping Assistance function on steering wheel should be limited and zero when driver applies torque more than some threshold
Safety_Goal_05	The Lane Departure Warning system must show the status of essential sensors and warn the driver of any discrepancy when switched on, so that driver may not rely completely on the system while driving

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	This Sensor responsible for capturing road images and provide them to the Camera Sensor ECU
Camera Sensor ECU	Electronic Control Unit (ECU) responsible for calculates the deviation from center lane and request for oscillation torque(LDW) wherever required.
Car Display	Displays status of (active/inactive) LDW & LKA function, thus informing the driver about the current status so that driver is well informed before any mishap happens
Car Display ECU	Electronic Control Unit (ECU) responsible for displaying status of (active/inactive) LDW & LKA function on the Car Display.
Driver Steering Torque Sensor	Sensor responsible for measuring the torque applied on driver wheel, this calculation is based on the signals received.
Electronic Power Steering ECU	Electronic Control Unit (ECU) responsible for

	calculating extra torque need to be applied for LKA function and vibrates steering wheel when LDW is activated.
Motor	An electric motor that applies the torque indicated by the Electronic Power Steering ECU 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	The Lane Departure Warning function applies a high amplitude oscillating torque(above limits)
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 a high frequency oscillating torque(above limits)
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 by time and number of times engaged, leading to

			potential misuse
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply limited torque when driver applies opposite torque above certain limit	NO	The Lane Keeping Assistance is not limited by torque amplitude, leading to accident in case an object suddenly comes in ego lane
Malfunction_05	Lane Departure Warning (LDW) function shall be deactivated when not able to find lanes on road and alert the driver	WRONG	The Lane Departure Warning function may give false alerts when used on roads with faded or missing lanes
Malfunction_06	The Lane Departure Warning (LDW) function shall be deactivated in case of any discrepancy with the system and alert the driver	WRONG	The Lane Departure Warning function does not monitor the state of the sensors and does not issue warning when required

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 (LDW) function shall ensure that amplitude of oscillating torque is less than Max_Torque_Amplitude	C	50 ms	Turn Off System
Functional Safety Requirement	The Lane Departure Warning (LDW) function shall ensure that frequency of oscillating torque is less than	C	50 ms	Turn Off System

01-02	Max_Torque_Frequency			
Functional Safety Requirement 01-03	The Lane Departure Warning (LDW) function shall be deactivated when any discrepancy in sensors or state of Camera Subsystem is Lane_Not_Found	A	50ms	Lane Departure Warning function is off

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 if Max_Torque_Amplitude is chosen such that it is detectable by the driver and does not cause the loss of steering	Verify that system turns off if torque amplitude ever exceeds Max_Torque_Amplitude
Functional Safety Requirement 01-02	Validate if Max_Torque_Frequency is chosen such that it is detectable by the driver and does not cause the loss of steering	Verify that system turns off if torque amplitude ever exceeds Max_Torque_Frequency
Functional Safety Requirement 01-03	Validate if Lane Departure warning function turns off when Lane_Not_Found is set	Verify that system turns off is Lane_Not_Found is set

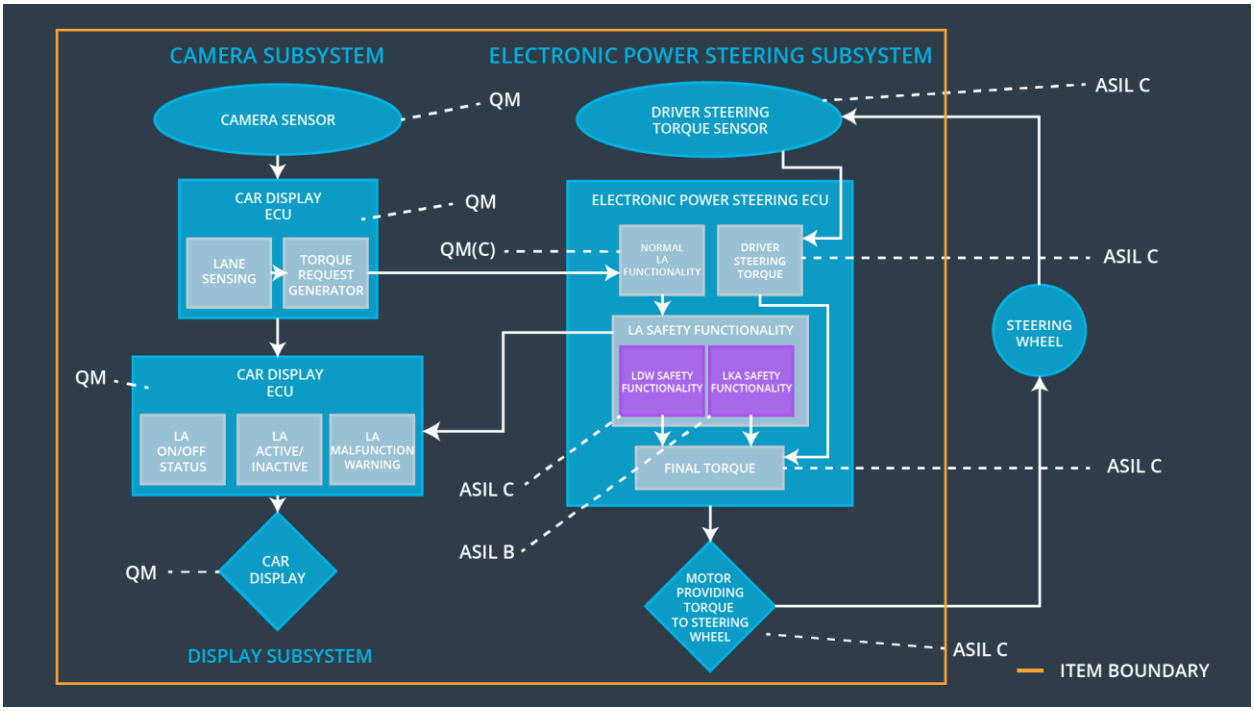
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The Lane Keeping Assistance (LKA) function must limit the number of times it engages to keep vehicle in lane	B	100ms	The Lane Keeping Assistance Torque is zero
Functional Safety Requirement 02-02	The Lane Keeping Assistance (LKA) function must limit the amplitude of torque it applies on steering wheel and disengage when driver applying opposite torque	B	50ms	The 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 if Lane Keeping Assistance function applies torque for duration Max_Duration, Max_Engage_Count number of times and zero torque threafter	Verify that the system outputs zero torque after Max_Duration and Max_Engage_Count is exceeded
Functional Safety Requirement 02-02	Validate if Lane Keeping Assistance sends zero torque to motor if Driver applies torque more than Max_Driver_Torque on steering wheel	Verify that Lane Keeping Assistance function sends zero torque when driver torque is more than Max_Driver_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 departure oscillating torque amplitude is below Max_Torque_Amplitude, this would be ensured by the lane keeping item.	**X**		
Functional Safety Requirement 01-02	The lane departure oscillating torque frequency is below Max_Torque_Frequency, this would be ensured by the lane keeping item.	**X**		
Functional Safety Requirement 02-01	The lane keeping assistance torque is applied for only Max_Duration, this would be ensured by the electronic power steering ECU.	**X**		
Functional Safety Requirement 02-02	When the camera sensors are not responding then electronic power steering ECU should be deactivated.	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked ?	Driver Warning
WDC-01	Turn off LDW functionality	Malfunction_01, Malfunction_02	Yes	Turn on warning light of the LDW functionality
WDC-02	Turn off LKA functionality	Malfunction_03, Malfunction_04	Yes	Turn on warning light of the LKA functionality