Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0
Released on 2018-05-22

Document history

Date	Version	Editor	Description
20-May-2018	0.1	Venkataraman	Initial Draft
22-May-2018	1.0	Venkataraman	First attempt

Table of Contents

Purpose of the Functional Safety Concept

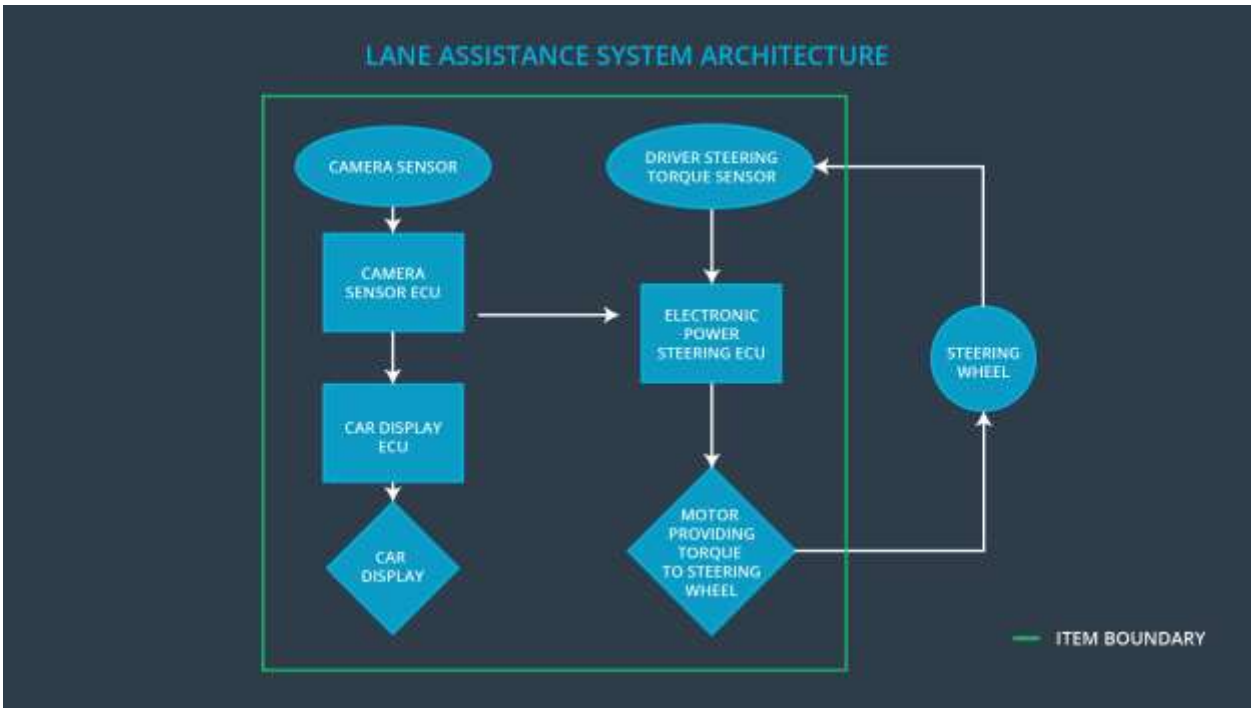
Identify the high level requirements without going into technical details and allocate them to different parts of the item architecture is the purpose of the functional safety concept. They must also be verified and validated.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The vibrating torque of steering wheel should be reduced to acceptable range.
Safety_Goal_02	The functional time of the LKA should be reduced.
Safety_Goal_03	The LDW function shall be turned off when driving on *off road conditions*.
Safety_Goal_04	The LKA function shall be deactivated when the camera sensor stopped working and driver should be warned about the deactivation (car dashboard)

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	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)
Car Display	Displays status of (active/inactive) LDW & LKA function.
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
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 an oscillating torque with very high torque amplitude. (above the 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 LKA function doesn't have any constrains that will prevent it from triggered falsely.
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply	WRONG	The lane keeping assistance function is

	the steering torque when active in order to stay in ego lane		activated randomly when camera sensor is not working.

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	Vibration torque amplitude below Max_Torque_Amplitude.
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	Vibration torque Frequency 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	Validate that the Max_Torque_Amplitude chosen is low enough that the driver does not loss control over the car and high enough to be detected by driver.	Verify that the system does turn off within a fault tolerant time interval, if Max_Torque_Amplitude is exceeded.
Functional Safety Requirement 01-02	Validate that the Max_Torque_Frequency chosen is low enough that the driver does not loss control over the car and high enough to be detected by driver.	Verify that the system does turn off within a fault tolerant time interval, if Max_Torque_Frequency is exceeded.

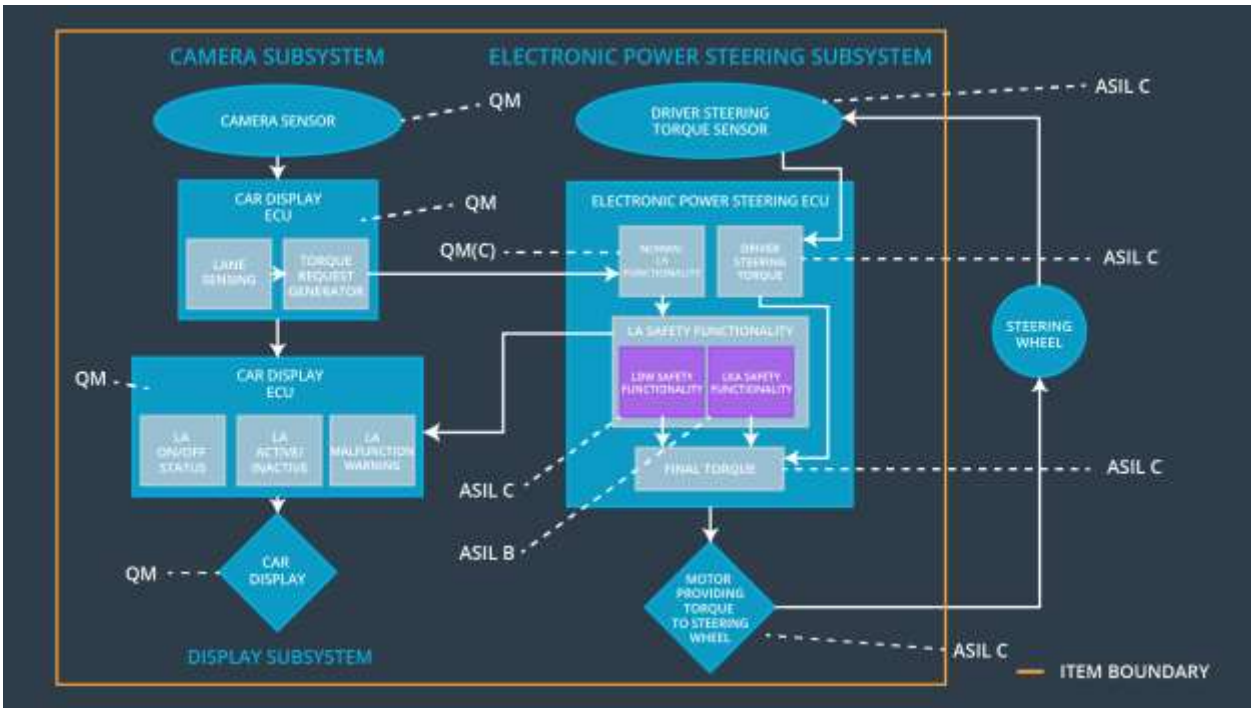
Lane Keeping Assistance (LKA) Requirements:

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 Assistant torque is zero
Functional Safety Requirement 02-01	The electronic power steering ECU shall be deactivated when the electronic power steering ECU detects the camera sensor is not working.	B	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 value chosen for Max_Duration dissuades drivers from taking their hands off the wheel.	Verify that the system does turn off within a fault tolerant time interval, if the lane keeping assistance ever exceeds Max_Duration
Functional Safety Requirement 02-02	Validate that Lane Keeping assistance shall be deactivated when the camera sensor stop working.	Verify that the system does turn off within a fault tolerant time interval, if the camera sensor stopped 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	**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 electronic power steering ECU 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 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