Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0
Released on 2018-06-21

Document history

Date	Version	Editor	Description
21-Jun-2018	1.0	Prathmesh Dali	Final Submission

Table of Contents

Purpose of the Functional Safety Concept

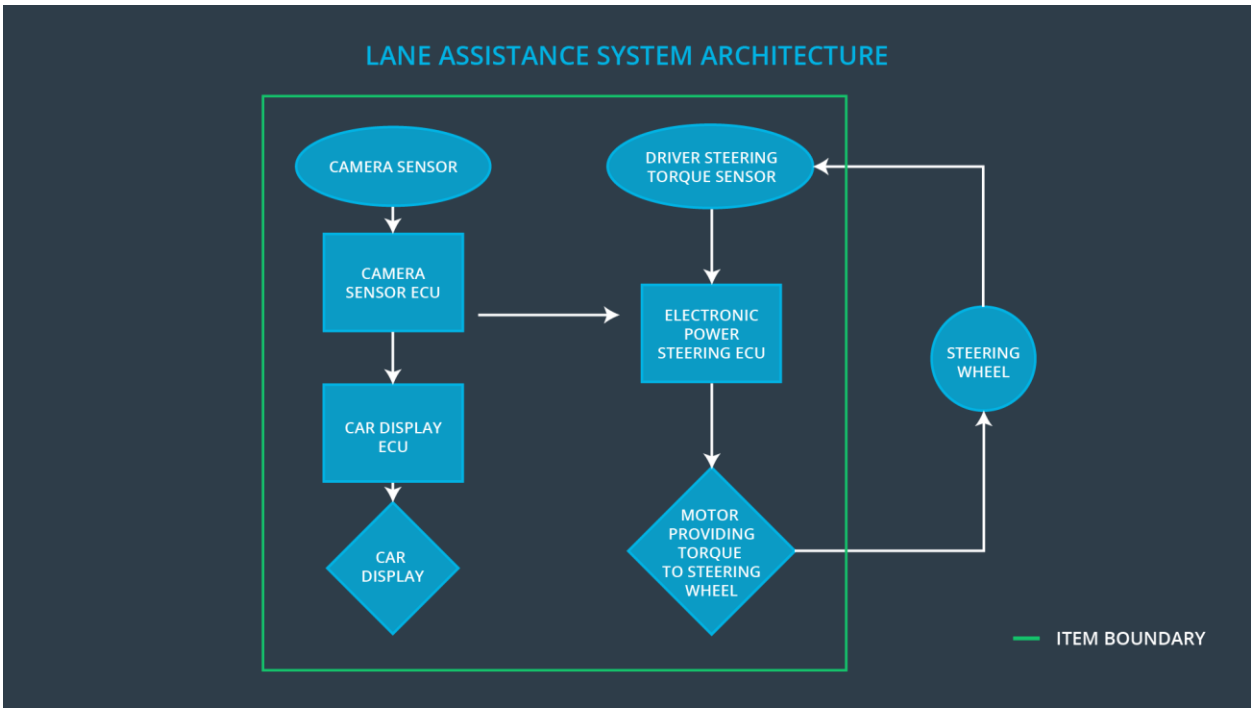
The purpose of Functional Safety Concept document is to identify the system high level requirements and allocate them to different parts of item architecture without going into technical detail. Finally, to prove that a system actually meets requirements, they have to be verified and validated. The information 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	Reduce the vibrating torque of the steering wheel to bring to the acceptance level.
Safety_Goal_02	Total functional time of the Lane Keeping Assistance shall be decreased.
Safety_Goal_03	While driving in the driving on off road conditions, the Lane Departure Warning function shall be turned off.
Safety_Goal_04	When there is no response from the camera sensors then the Lane Keeping Assistance function shall be deactivated driver shall be warned about the deactivation by displaying the issue on the car dashboard.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	This Sensor is responsible for capturing road images and provide them to the Camera Sensor Electronic Control Unit.
Camera Sensor ECU	ECU is responsible for calculating the deviation from the center lane and requesting for oscillation torque(LDW) wherever required.
Car Display	Displays status of LDW & LKA function whether they are active or inactive and thus informing the driver about the current status so that the driver is well informed before anything happens
Car Display ECU	ECU is responsible for displaying status of LDW & LKA function whether they are active or inactive
Driver Steering Torque Sensor	This sensor measures the torque applied to the steering wheel.
Electronic Power Steering ECU	It is required to calculate extra torque which needs to be applied for LKA function and vibrates steering

	wheel when LDW is activated.
Motor	It interprets the EPS ECU data for controlling 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	Lane Departure Warning function applies oscillating torque of a very high amplitude.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	Lane Departure Warning function applies oscillating torque of a very high frequency.
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	LKA function has a time limiting function which results in misuse of autonomous driving function.

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 less than Max_Torque_Amplitude value.	C	50 ms	Turn off LDW
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is less than Max_Torque_Frequency value	C	50 ms	Turn off LDW

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 the value of **Max_Torque_Amplitude** such that it is adequate enough send warning to the driver without causing steering loss.	Validate whether the system is turned off when Max_Torque_Amplitude exceeds within 50ms of fault tolerant.
Functional Safety Requirement 01-02	Choose the value of **Max_Torque_Frequency** such that it is enough to send the warning driver without causing steering loss.	Validate whether the system is turned off when Max_Torque_Amplitude exceeds the fault tolerant limits.

Lane Keeping Assistance (LKA) Requirements:

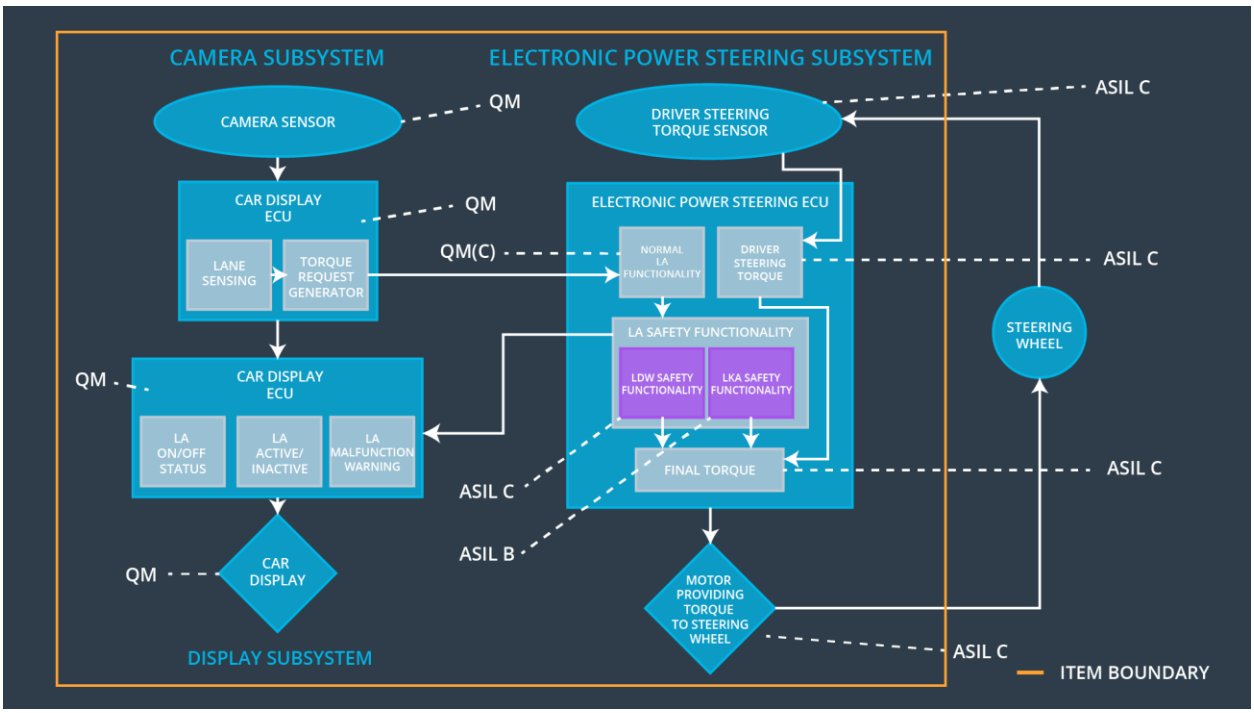
ID	Functional Safety Requirement	ASI	Fault Tolerant Time	Safe State

		L	Interval	
Functional Safety Requirement 02-01	The electronic power steering Electronic Control Unit shall ensure that the LKA torque is applied only for Max_Duration value	B	500 ms	Turn Off LKA

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 whether Lane Keeping Assistance is active until the Max_Duration is reached and after that warning light is turned on.	Lane Keeping Assistance is turned off once the Max_Duration is reached

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 warning torque amplitude is less than Max_Torque_Amplitude	X		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure warning torque frequency is less than Max_Torque_Frequency	X		
Functional Safety Requirement 02-01	Test if Lane Keeping Assistance is active until the Max_Duration is reached and post warning light turns on.	X		

Warning and Degradation Concept

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