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
18-5-2018	1.0	Atul Singh	First Attempt

Table of Contents

[Instructions: We have provided a table of contents. If you change the document structure, please update the table of contents accordingly. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Purpose of the Functional Safety Concept

[Instructions: Answer what is the purpose of a functional safety concept?]
The purpose of functional safety is to identify safety requirements and then allocate those requirements to different parts of the item architecture. It looks at the general functionality of the item without going into its technical details.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

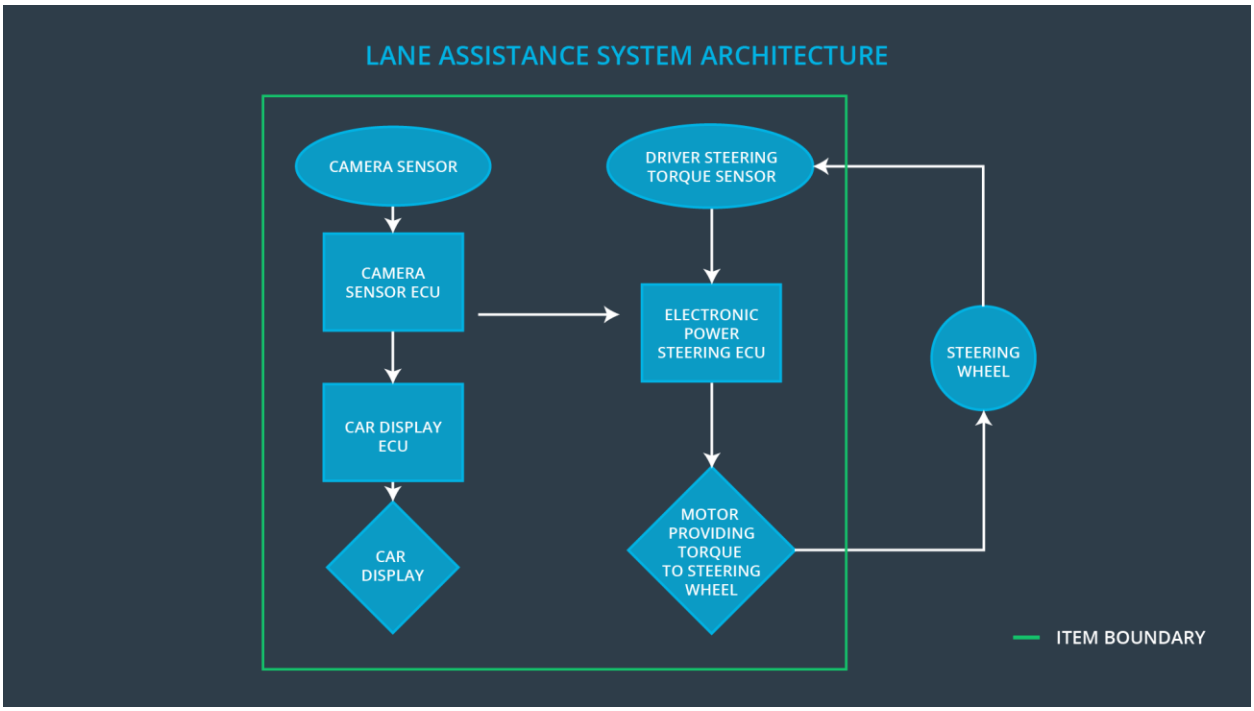
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

OPTIONAL:
If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.
]

ID	Safety Goal
Safety_Goal_01	Lane Departure Warning(LDW) should provide a limited amount of oscillating steering torque.
Safety_Goal_02	Lane Keep Assistance should be time limited so that driver cannot misuse the system for autonomous driving

Preliminary Architecture

[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]



Description of architecture elements

[Instructions: Provide a description for each of the item elements; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	Provides lane images to the Camera Sensor ECU
Camera Sensor ECU	Checks whether the car is leaving the lane or is in the lane by going through the image provided by the camera sensor .
Car Display	It is uses to display warnings to the driver
Car Display ECU	It is responsible for the warnings that are displayed by the car Display. The warning can be for the activation and deactivations for LKA and LDW.
Driver Steering Torque Sensor	Measure the torque applied by the driver on the steering wheel by the driver.
Electronic Power Steering ECU	It process the inputs from Camera Sensor ECU and Driver Steering Torque Sensor to produce a torque that is transferred to the steering wheel motor to provide Lane Assistance Functionality

Motor	Receives the torque from the ECU and applies it 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

[Instructions: Fill in the functional safety analysis table below.]

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 torque amplitude provided by lane departure warning function may be very high(above limit)
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The torque amplitude provided by lane departure warning function may be very high (above limit)
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	Since the LKA is not limited to a time duration, the driver may misuse it as an autonomous driving function.

Functional Safety Requirements

[Instructions: Fill in the functional safety requirements for the lane departure warning]

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	ECU should make sure that the oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Lane Assistance functionality is kept in off state
Functional Safety Requirement 01-02	ECU should make sure that the oscillating torque frequency is below MAX_Torque_Frequency	C	50 ms	Lane Assistance functionality is kept in off state

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	The MAX_Torque_Amplitude is chosen high enough to be detected by the driver and low enough so that the driver may not lose control	As the MAX_Torque_Amplitude is crossed the system output should be set to zero
Functional Safety Requirement 01-02	The MAX_Torque_Fequency is chosen high enough to be detected by the driver and low enough so that the driver may not lose control	As the MAX_Torque_Amplitude is crossed the system output should be set to zero

[Instructions: Fill in the functional safety requirements for the lane keeping assistance]

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	A	Fault	Safe State

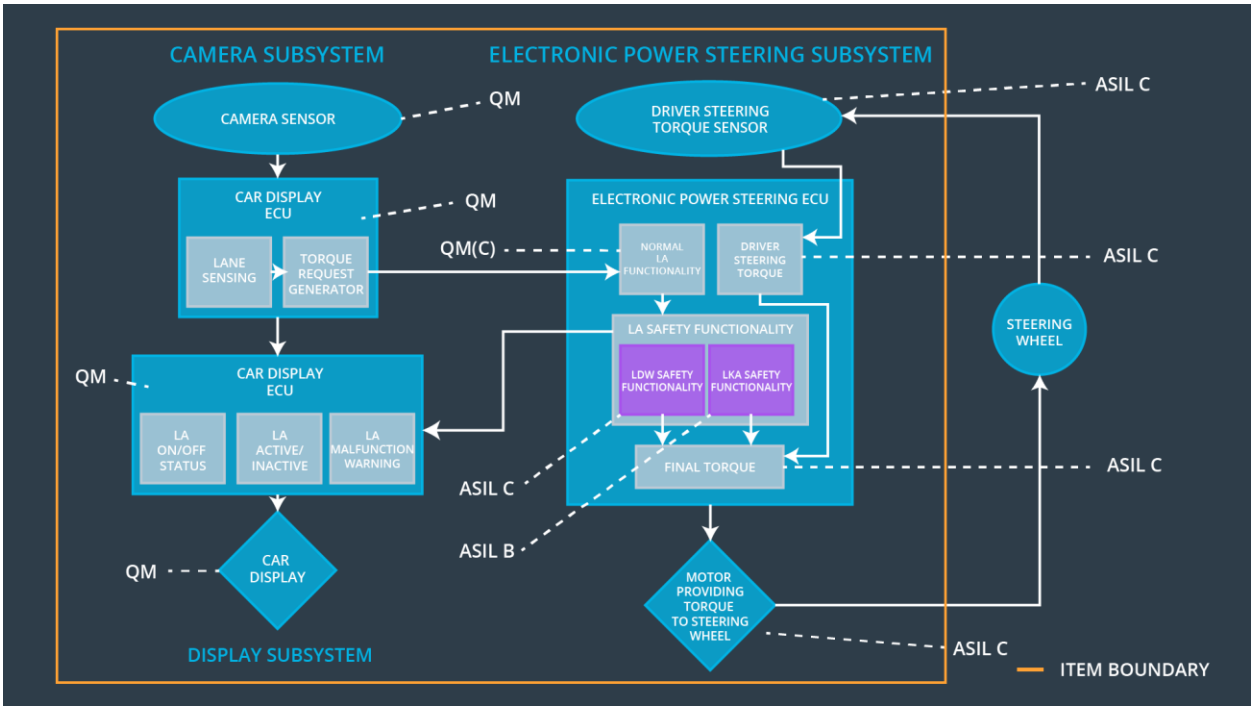
		SIL	Tolerant Time Interval	
Functional Safety Requirement 02-01	It should be ensured by the electronic power steering ECU that the torque is applied only for Max_Duration	B	500ms	Lane Assistance functionality is not activated

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.	The lane keep assistance system should turn off if max_duration is exeeded

Refinement of the System Architecture

[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the functional safety lesson including all of the ASIL labels.]



Allocation of Functional Safety Requirements to Architecture Elements

[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	It should be ensured by the electronic power steering ECU that the torque is applied only for Max_Duration	**X**		
Functional Safety Requirement 01-02	ECU should make sure that the oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 02-01	ECU should make sure that the oscillating torque frequency is below MAX_Torque_Frequency	**X**		

Warning and Degradation Concept

[Instructions: Fill in the warning and degradation concept.]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off lane assistance functionality	Malfunction_01	Yes	Car Displays shows the Lane Assistant Malfunction Warning

WDC-02	Turn off lane assistance functionality	Malfunction_02	Yes	Car Displays shows the Lane Assistant Malfunction Warning