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
August 13, 2018	V 1.0	Li Gen	

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?]
Functional safety concept define what vehicle needs to do, and define a higher level new requirements and allocate these requirements to system diagrams.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

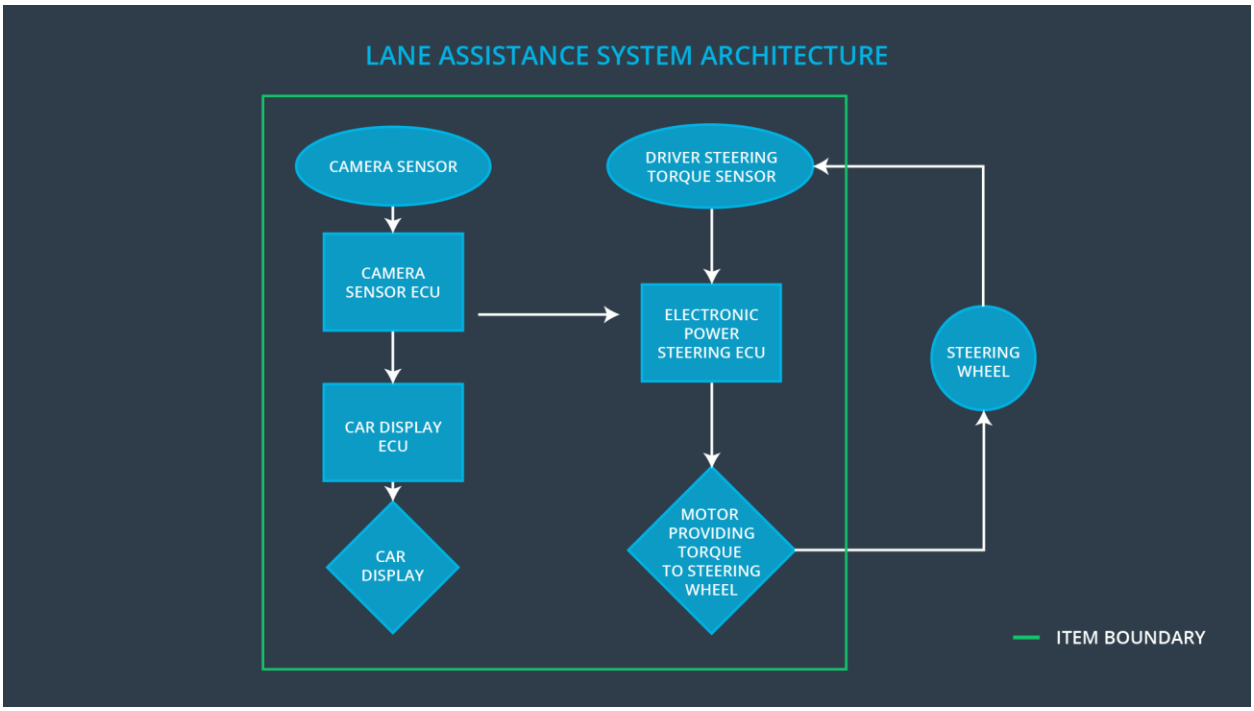
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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

ID	Safety Goal
Safety_Goal_01	the oscillating steer torque from the LDW should be limited
Safety_Goal_02	the LDA function shall be time limited and the additional steering torque shall end after a given time interal.

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	Hardware that get pattern information
Camera Sensor ECU	Analysis pattern information and output result to car display ECU and EPS ECU.
Car Display	Shower warning information based on signal from car display ECU
Car Display ECU	Calculate whether display warning information and output to car display.
Driver Steering Torque Sensor	Sensor which measure steering torque, and output its result to EPS ECU.
Electronic Power Steering ECU	Receive information from camera sensor ECU and driver steering torque sensor, after calculation and output signal to motor of steering wheel.
Motor	Output torque to steering wheel based on EPS ECU

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 LDW function provide applies an oscillating steering torque with very high torque amplitude.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	more	The LDW function provide applies an oscillating steering torque with very high torque frequency.
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	no	The LDA function has a no time limits which may lead to misuse 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	The LDW item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Set the oscillation torque amplitude to zero
Functional Safety Requirement 01-02	The LDW item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Set the oscillation torque amplitude to zero

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	Test how drivers react to different torque amplitudes, and choose an appropriate value.	When the torque amplitude crosses the limit, the lane assistance output is set to zero within 50ms fault tolerant time interval.
Functional Safety Requirement 01-02	Test how drivers react to different torque frequency, and choose an appropriate value.	When the torque frequency crosses the limit, the lane assistance output is set to zero within 50ms fault tolerant time interval.

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

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The LKA function item shall be time limiter and the additional steering torque shall end after a given time interval so that the driver	B	500ms	Set the steering torque to zero

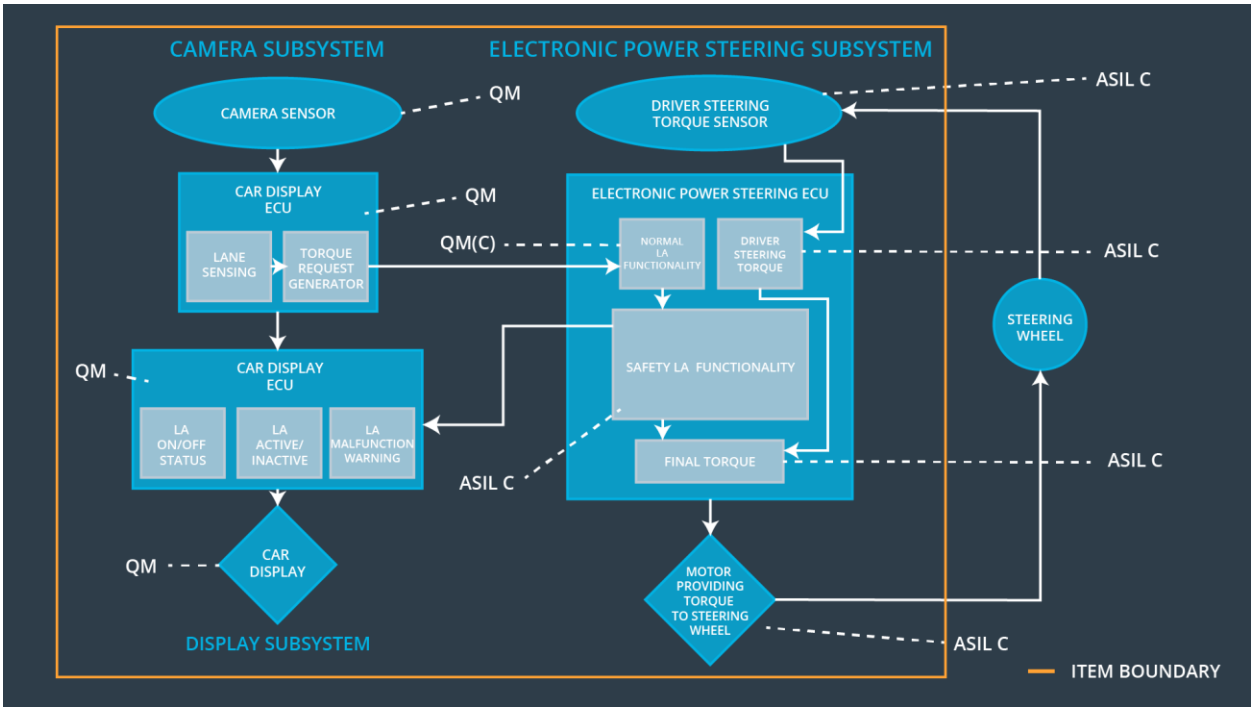
	can not misuse the system for autonomous driving.			

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 that max_duration chosen really did dissuade drivers from taking their hands off the wheel.	The LDA function whether does turn off if the LKA every exceeded max_duration.

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	The electronic power steering ECU shall ensure that the oscillating steering torque is below Max_Torque_Amplitude	√		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the oscillating steering frequency is below Max_Torque_Frequency	√		
Functional Safety Requirement 02-01	electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	√		

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	The LDW system turn off	The steering wheel ECU receive a vibrational torque request beyond the allowed	yes	A warning light will turn on

		maximum		
WDC-02	The LKA system turn off	The steering wheel ECU receive steering wheel torque is zero from driver for a limited time	yes	A warning light will turn on