Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.3

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
30/09/2017	1.0	ZEESHAN ANJUM	First Attempt
04/10/2017	1.1	ZEESHAN ANJUM	Safety Goals Update
12/10/2017	1.2	ZEESHAN ANJUM	Review
24/10/2017	1.3	ZEESHAN ANJUM	Update after 1st submission review

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 functional safety concept provides a high-level overview of the system. Based on the hazard analysis and risk assessment

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

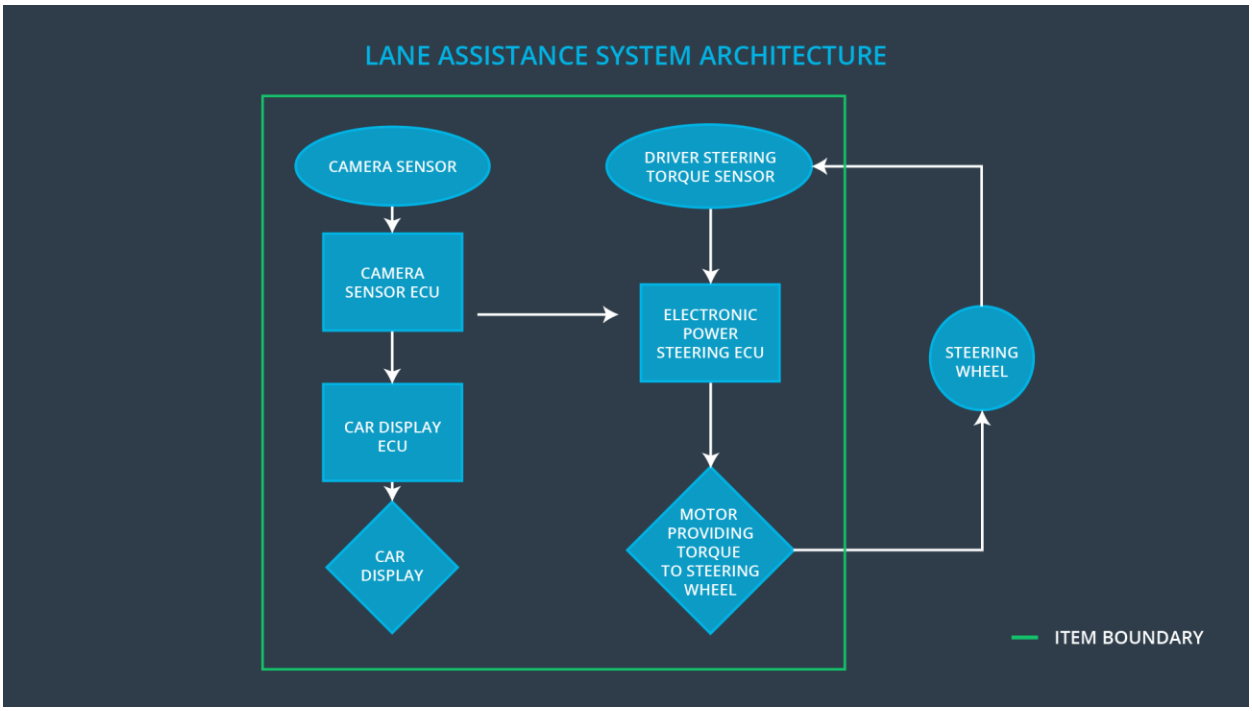
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 torque (amplitude & frequency) to the steering wheel from the lane departure warning function shall be limited.
Safety_Goal_02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only limited duration.
Safety_Goal_03	The camera ECU shall send signal to Car Display ECU if LKA is activated or not
Safety_Goal_04	The LKA function shall stop when camera will unable to detect road markings and notify to driver

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	The camera sensor reads in images from the road.
Camera Sensor ECU	The camera sensor ECU identifies when the vehicle has accidentally departed its lane, and send the appropriate message to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	Dashboard to display various warning information to let the driver know about lane departure malfunction
Car Display ECU	The camera ECU after detecting a lane departure will request a warning light to turn on the car display through car display ECU
Driver Steering Torque Sensor	Measures the torque provided by the driver
Electronic Power Steering ECU	Responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request and finalize the steering torque request to the Motor

Motor	Provides torque 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 lane departure warning function applies an oscillating torque with very high torque amplitude (above 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 lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function

Malfunction_04	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	NO	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	The LKA function is not able to detect lane in low illumination

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 EPS ECU shall ensure that the lane departure warning torque amplitude is below Max_Torque_Amplitude	C	50ms	Set vibration torque to zero
Functional Safety Requirement 01-02	The EPS ECU shall ensure that the lane departure warning torque frequency is below the Max_Torque_Frequency	C	50ms	Set vibration torque to zero

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety	Test how drivers react to different torque amplitudes to prove that we chose an	Verify that the safety requirement is met when the torque amplitude

Requirement 01-01	appropriate value	crosses the limit, the lane assistance output is set to zero within the 50ms fault tolerant time interval
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that we chose an appropriate value	Verify that the safety requirement is met when the torque frequency crosses the limit, the lane assistance output is set to zero within the 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 electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	Set lane keeping assistance torque to zero
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU stops detecting road markings and shall send its off status to the Car Display.	B	500ms	Set lane keeping assistance torque to zero

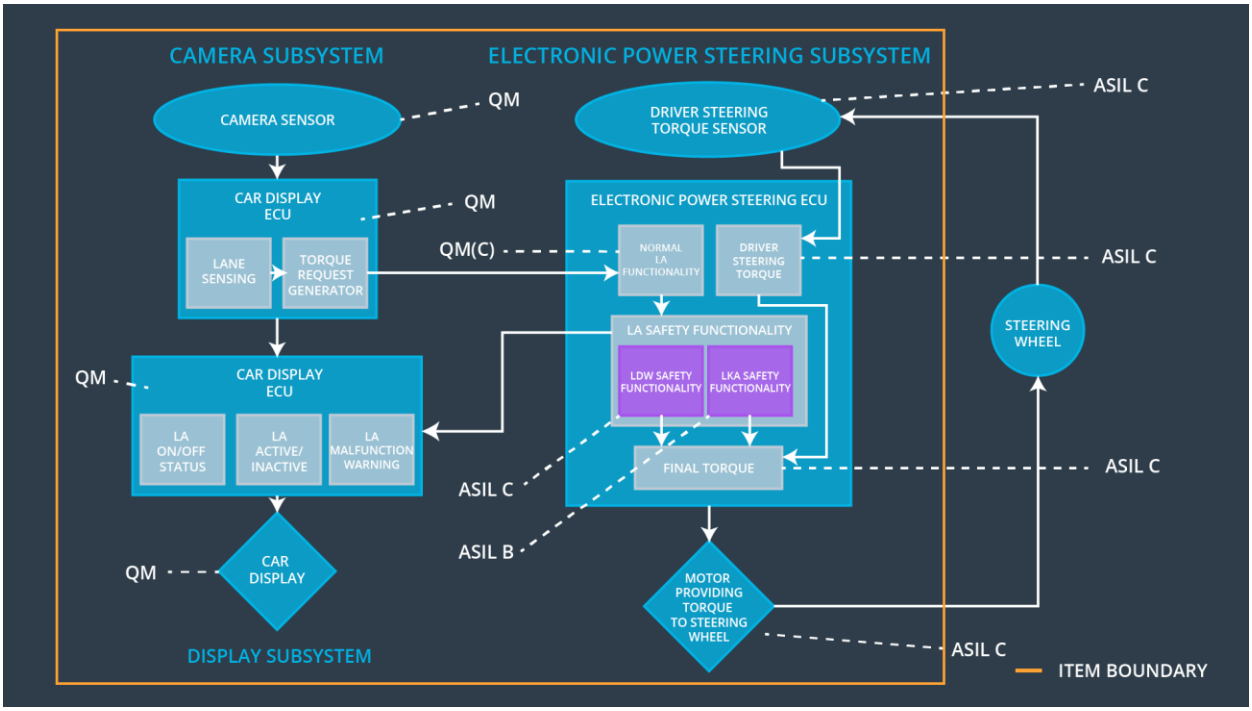
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-01	Validate that the Max_Duration chosen discourages drivers from taking their hands off the wheel	Verify that the lane keeping assistance shuts off if lane keeping exceeds Max_Duration
Functional Safety	Validate Camera sensor ECU does not generate torque requests when lane	Verify that the system really does turn off if the camera sensor ECU stop road

Requirement 02-02	sensing is lost	marking detection

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	The lane keeping item shall ensure that the lane departure	✓		

01-01	oscillating torque amplitude is 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	✓		
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for 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	Turn Off	Oscillating torque amplitude is above Max_Torque_ Amplitude and oscillating torque frequency is above Max_Torque_Fr equency	Yes	Car Display
WDC-02	Turn Off	Lane keeping assistance torque is applied for longer than Max_Duration	Yes	Car Display