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
2019-01-30	1.0	Vern Francisco	1st attempt at completing the assignment

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 the Functional Safety Concept is to avoid accidents by reducing risk to acceptable levels. The Functional Safety Concept reduces risk by doucmenting functional safety

requirements derived from safety goals and allocates the requirement to the appropriate place in the architecture.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

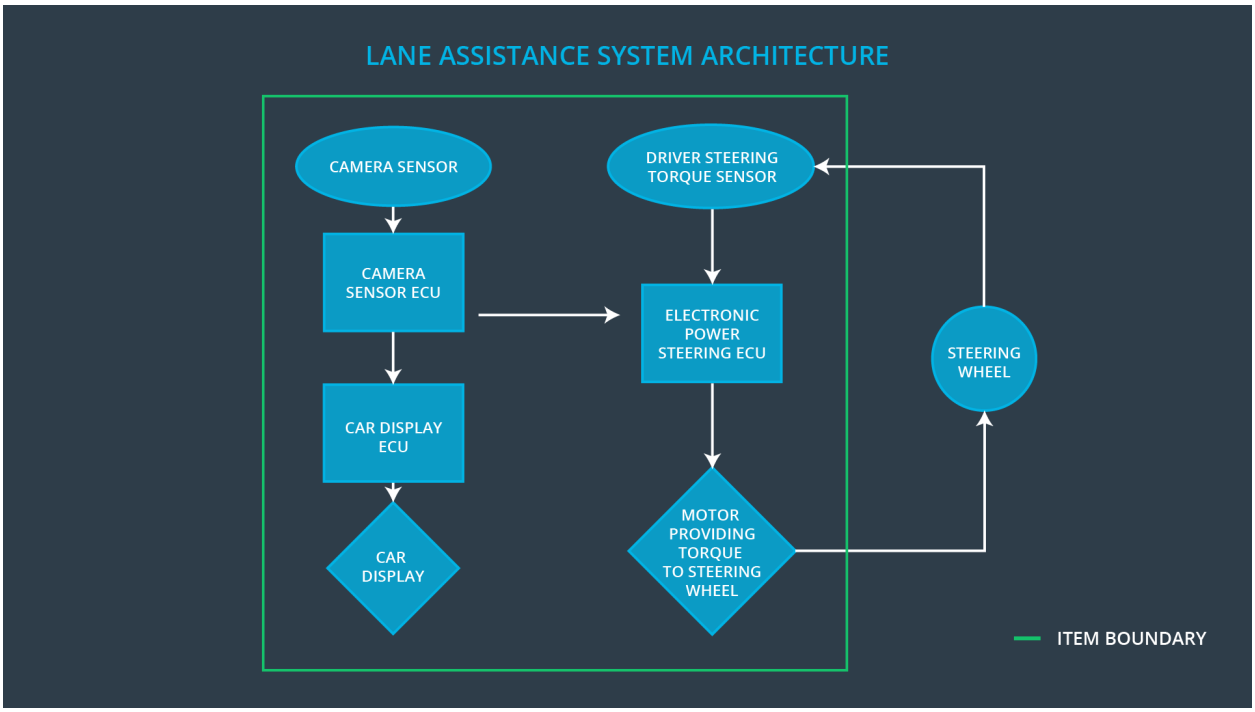
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 to the steering wheel from teh lane departure function shall be limited
Safety_Goal_02	**The land keeping assistance function shall be time limited and the additional steering torque shall end after a given time interval so that the 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	Responsible for detecting lane lines and other objects in the road
Camera Sensor ECU	Determines when the vehicle leaves the lane by mistake by processsing images from the camera sensor. It senses the lane and creates a torque request for the Electronic Power Steering ECU
Car Display	Informs the driver of vehicle status and warnings
Car Display ECU	Takes input from the Camera Sensor ECU and other ECUs and generates commands to activate lights and guages in the car display: It controls a light that shows the on/off status of the Lane Assistance system and a light showing whether the Lane Assistance system is active or inactive
Driver Steering Torque Sensor	Senses the torque that the driver is imparting on the steering wheel
Electronic Power Steering ECU	The Electronic Power Steering ECU receives the

	torque request from the camera sensor ECU and receives information about the driver's steering torque. It adds these torque values and sends the final torque request to the Motor
Motor	Adds torque to the steering wheel

Functional Safety Concept

The functionalncept 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.

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 lane keeping item shall ensure that he lane departure oscillating toqrue ampliteude is below Max_Torque_Amplitude	C	50ms	System is turned off
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is belwo Max_Torque_Frequency	C	50ms	System is turned off

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	On a closed course with a test driver, change the maximum amplitude until the driver can safely recover control of the vehicle when an oscillation is induced	Set the max amplitude at the desired level. Then force a oscillatory torque input with a magnitude greater than the max amplitude. Verify that the system does indeed shut down when the maximum amplitude has been exceeded
Functional Safety Requirement 01-02	On a closed course with a test driver, change the maximum frequency until the driver can safely recover control of the vehicle when an oscillation is induced	Set the max frequency at the desired level. Then force a oscillatory torque input with a frequency greater than the max frequency. Verify that the system does indeed shut down when the maximum frequency has been exceeded

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

Lane Keeping Assistance (LKA) Requirements:

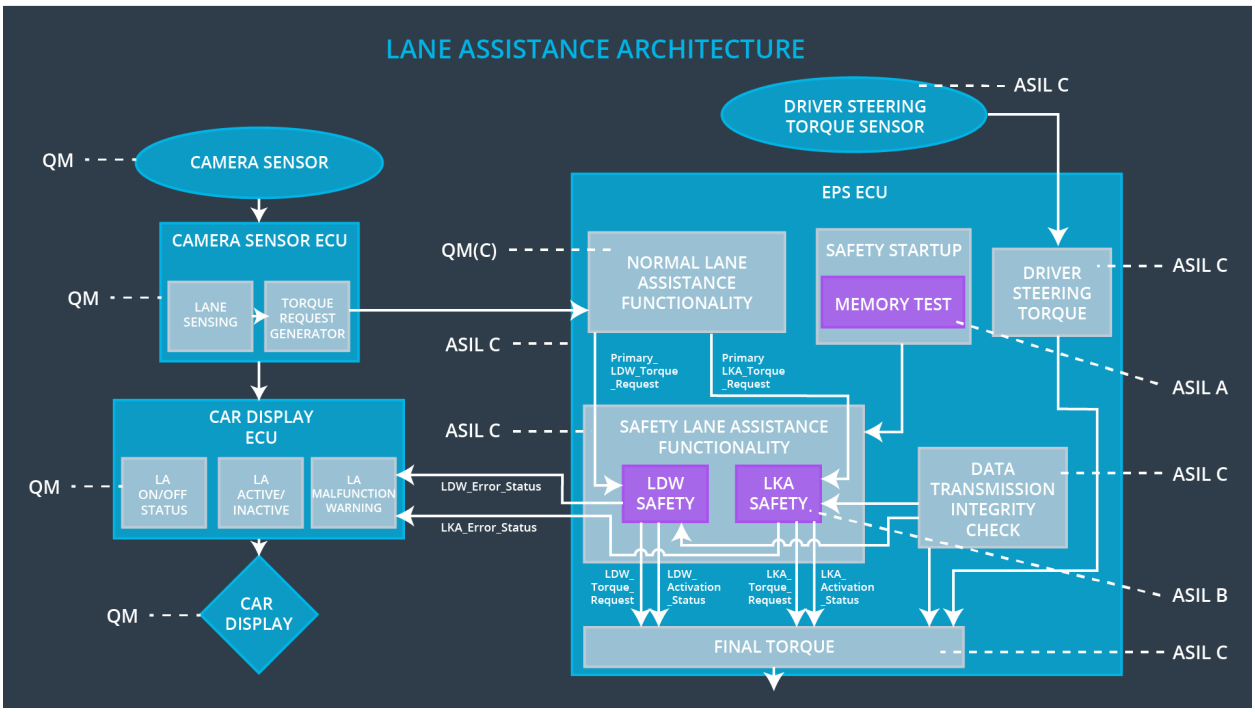
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only a Max_Duration	B	500ms	System is turned off

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	Criteria: Drivers have been significantly dissuaded from taking their hands off the wheel. Method: On a closed course, try different durations for cancellation to see when drivers would become most dissuaded to remove their hands from the steering wheel	Set the max duration to the value judged to help dissuade drivers. On a closed course, ask a test driver to remove his/her hands from the steering wheel. Then verify that the system does in fact turn off after the max duration has been achieved

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 he lane departure oscillating toqrue ampliteude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure tha the lane departure oscillating torque frequency is below Max_Torque_Frequency	**X**		
Functional	The electronic power steering	**X**		

Safety Requirement 02-01	ECU shall ensure that the lane keeping assistance torque is applied for only a 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 the lane departure warning function	The frequency of the oscillating torque or the magnitude of the oscillating torque have exceeded their limits	Yes	Warning Light
WDC-02	Turn off the lane keeping assistance function	The max duration of driver hands off the wheel has been exceeded	Yes	Warning Light