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
9/22/2018	1.0	George V. Paul	First draft

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?]

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

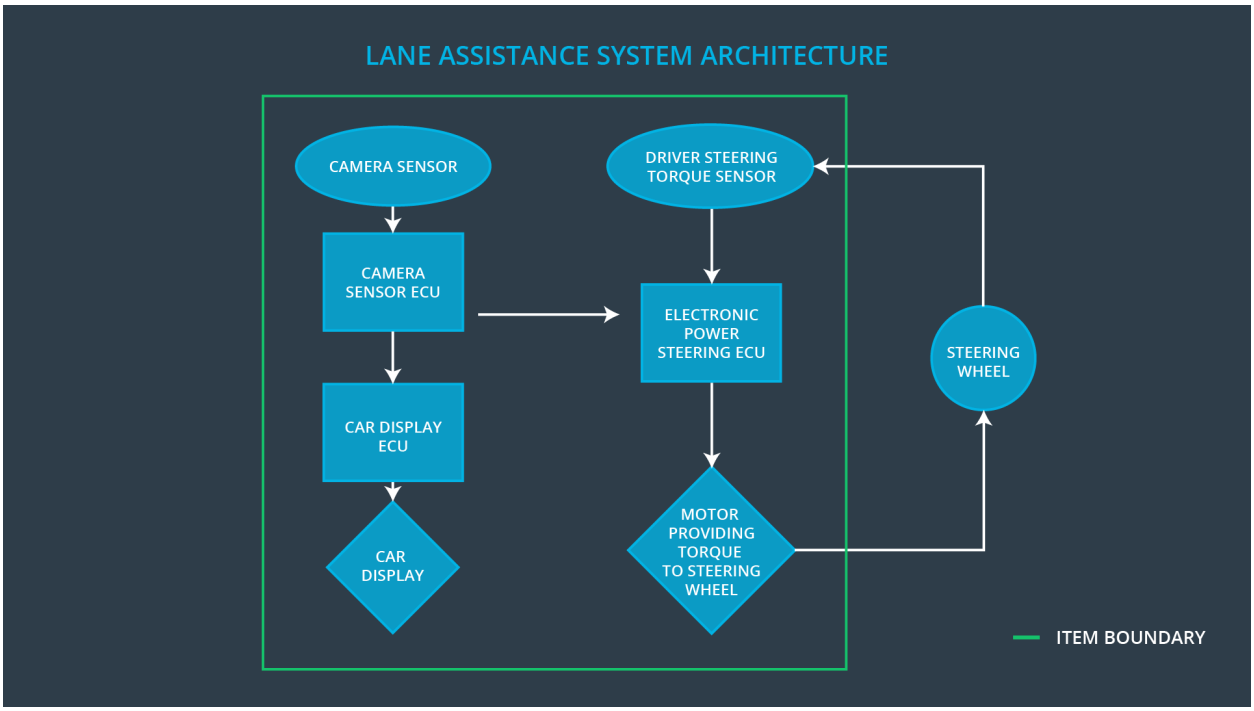
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 steering torque from the lane departure warning function shall be limited
Safety_Goal_02	The lane 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	The Camera Sensor captures images of the road and detects the driving lane lines.
Camera Sensor ECU	The Camera Sensor ECU identifies when the vehicle has accidentally departed from its lane and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	The Car Display shows the warnings when the LDW system senses a malfunction or fault.
Car Display ECU	The Car Display ECU receives the messages from the LDW system about its on/off state. It also displays the LDW system malfunctions by translating them into warning lights and sounds.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor senses the human driver's input and relays it to the Electronic Power Steering ECU.
Electronic Power Steering ECU	The Electronic Power Steering ECU takes as input

	both the Driver Steering torque readings and the Camera Sensor ECU torque readings and combines them and sends the resulting torque signal to the steering wheel motor.
Motor	The motor is the last element of the LDW system and converts the torque readings to the actual torque on the steering wheel of the car.

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 oscillating torque magnitude is above a safe limit for the driver.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The oscillating torque frequency is above a safe limit for the driver to keep the car under control.
Malfunction_03	Lane Keeping Assistance (LKA)	NO	The LKA system stays active beyond a

	function shall apply the steering torque when active in order to stay in ego lane		time limit which can lead to the driver using it as an autonomous 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 system shall ensure that the magnituge of the oscillating torque from the warning system is below the Max_Torque_Amplitude.	C	50ms	Set the oscillating torque signal to 0.
Functional Safety Requirement 01-02	The LDW system shall ensure that the frequency of the oscillating torque from the warning system is below the Max_Torque_Frequency.	C	50ms	Set the oscillating torque signal to 0.

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 the response of actual drivers to different magnitudes of torque vibrations.	Verify that the LDW system output is 0 when the oscillating torque amplitude goes beyond the tested limit.
Functional Safety Requirement 01-02	Test the response of actual drivers to different frequencies of torque vibrations	Verify that the LDW system output is 0 when the oscillating torque frequency goes beyond the tested limit.

[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 limit the time that the LKA system is active	B	500ms	Set the torque from LKA to 0.

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 the max_duration that drivers take to stop paying attention to the road when the LKA system is active.	Verify that the torque from LKA is set to 0 when the LKA system is active beyond 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**Yes**	**No**	**No**
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**Yes**	**No**	**No**
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the LKA torque shall be applied only for Max_Duration.	**Yes**	**No**	**No**

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	LDW function is switched off.	Malfunction_01 Malfunction_02	Yes	Malfunction warning with the LDW indicator on.
WDC-02	LKA function is switched off.	Malfunction_03	Yes	Malfunction warning with the LKA indicator on.