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
19-05-2018	1.0	Hitesh C	Initial 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?]

Functional Safety looks at the system from a higher level without delving into the technical details of the system. The primary focus here is to reduce the risks to below the societal accepted levels.

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 system shall be time limited, thus after a lane keeping manoeuvre, the control is given back to the driver

Preliminary Architecture

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

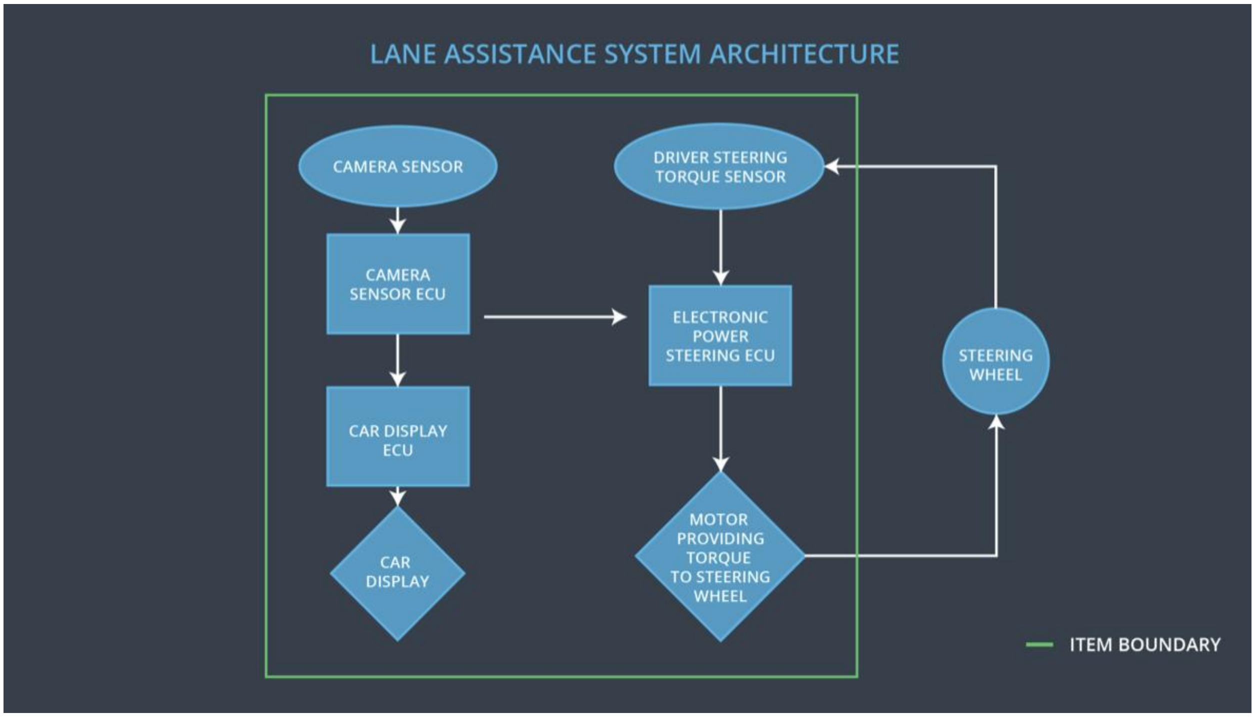

LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

Fig 1. Preliminary Architecture of Lane Assistance System

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	Capture images and provide them to the camera sensor ECU continuously
Camera Sensor ECU	Detect Lane Lines and calculate the position of the car with respect to the lanes
Car Display	Display the status of the systems and also warnings when a system malfunctions
Car Display ECU	It controls the things displayed on the car display in accordance with the inputs received from other systems.
Driver Steering Torque Sensor	It measures the torque applied to the steering wheel.
Electronic Power Steering ECU	It takes input from Driver Steering Torque Sensor and camera ECU and decides on the amount of torque needed to be applied on the steering wheel
Motor	The Motor is actuated by the input from Electronic

	Power Steering ECU. It applies the requisite 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 Amplitude of Applied Oscillating torque is too high
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The Frequency of Applied Oscillating torque is too high
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	The LKA doesn’t have a time limiting function resulting in its misuse as autonomous driving mode

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 the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Turn of the LDW functionality
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Turn of the LDW functionality

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 quantum of Max_Torque_Amplitude is chosen such that it is adequate enough to warn the driver and low enough to not cause steering loss.	Validate whether the system turns off when Max_Torque_Amplitude is exceeded.
Functional Safety Requirement 01-02	The quantum of Max_Torque_Frequency is chosen such that it is adequate enough to warn the driver and low enough to not cause steering loss.	Validate whether the system turns off when Max_Torque_Frequency is exceeded.

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

Lane Keeping Assistance (LKA) Requirements:

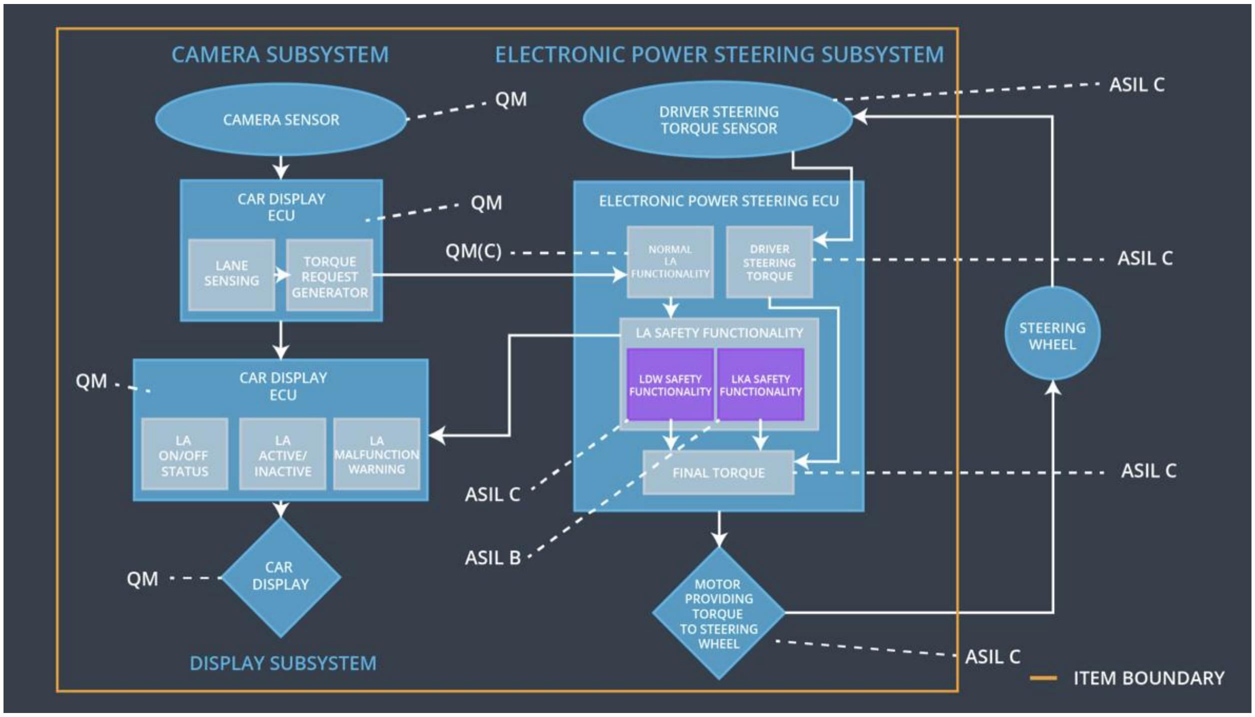
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	LKA Function will be time limited for a Max_Duration	B	500 ms	Set the LKA torque to zero

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	Test and validate that the max_duration chosen is large enough to bring back the vehicle to the center of the lane and small enough to discourage driver taking hands off the steering wheel	Verify that the LKA function turns off when the Max_Duration is exceeded

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 amplitude of Lane Departure Warning oscillating torque is below Max_Torque_Amplitude	**Responsible**	**Not Responsible**	**Not Responsible**

Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the Frequency of Lane Departure Warning oscillating torque is below Max_Torque_Frequency	**Responsible**	**Not Responsible**	**Not Responsible**
Functional Safety Requirement 02-01	The Electronic Power Steering Shall ensure that the Lane Keeping Torque is applied for a maximum duration of Max_Duration	**Responsible**	**Not Responsible**	**Not Responsible**

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 Functionality	Malfunction_01 Malfunction_02	Yes	Warning Light on Dashboard and warnings displayed on car display
WDC-02	Turn OFF the Functionality	Malfunction_03	Yes	Warning Light on Dashboard and warnings displayed on car display