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
3/12/2018	0.5	Tan Wang	First Draft
3/13/2018	0.6	Tan Wang	Added the refined architecture diagram
3/19/2018	1.0	Tan Wang	First Submission

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 is a document that aims to analyze the subsystems and allocate risk level to each subsystem at a high-level view, so that it can facilitate the process to avoid accidents by reducing risk to acceptable levels.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

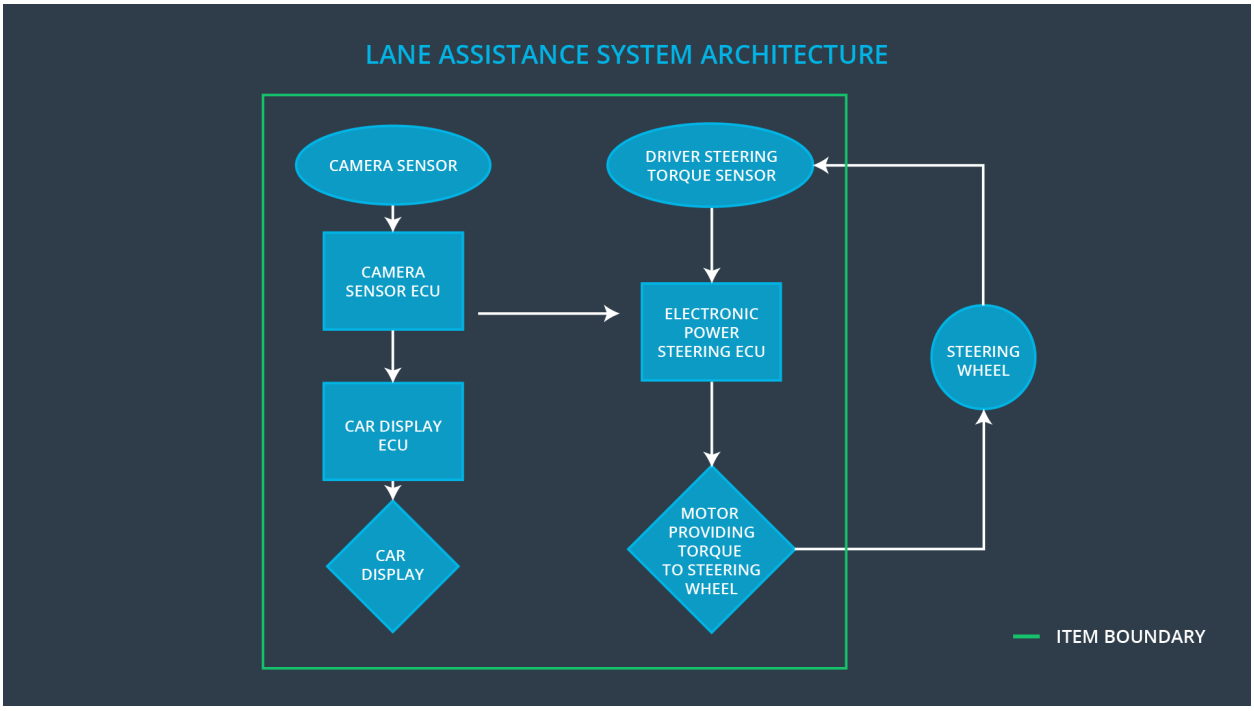
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 waring 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]



Camera Subsystem:

- Camera Sensor
- Camera Sensor ECU

Car Display:

- Car Display ECU
- Car Display

Electronic Power Steering system:

- Driver Steering Torque Sensor
- Electronic Power Steering ECU
- Motor

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	Gets visual perception (images and videos) of the environment
Camera Sensor ECU	Extracts lane lines from sensor images and calculates the real world position of lane lines, and generate torque requests to further components

Car Display	Presents status information and warnings to drivers
Car Display ECU	Converts status and error data from other components into displays
Driver Steering Torque Sensor	Gets the torque applied to the steering wheel by drivers
Electronic Power Steering ECU	Calculates the torque required to keep the car in lane
Motor	Applies torque to the steering wheel when the car is drifting away from the lane by mistake

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	MORE	The lane departure warning function applies an oscillating torque with very high torque frequency (above limit)

	feedback		
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 the lane departure oscillating torque amplitude is below max_torque_amplitude	C	50ms	The oscillating torque amplitude is set to 0
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below max_torque_frequency	C	50ms	The oscillating torque frequency is set 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	Testing how drivers react to different torque amplitude, make sure drivers could acknowledge the warning and still be able to operate steering wheel normally without too much discomfort	Inserting a software fault that triggers a steering torque over the maximum amplitude, and check whether the output torque can be set to 0 in 50ms during software testing

Functional Safety Requirement 01-02	Testing how drivers react to different torque frequency, make sure drivers could acknowledge the warning and still be able to operate steering wheel normally without too much discomfort	Inserting a software fault that triggers frequent steering torques over the maximum frequency, and check whether the output torque can be set to 0 in 50ms during software testing

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

Lane Keeping Assistance (LKA) Requirements:

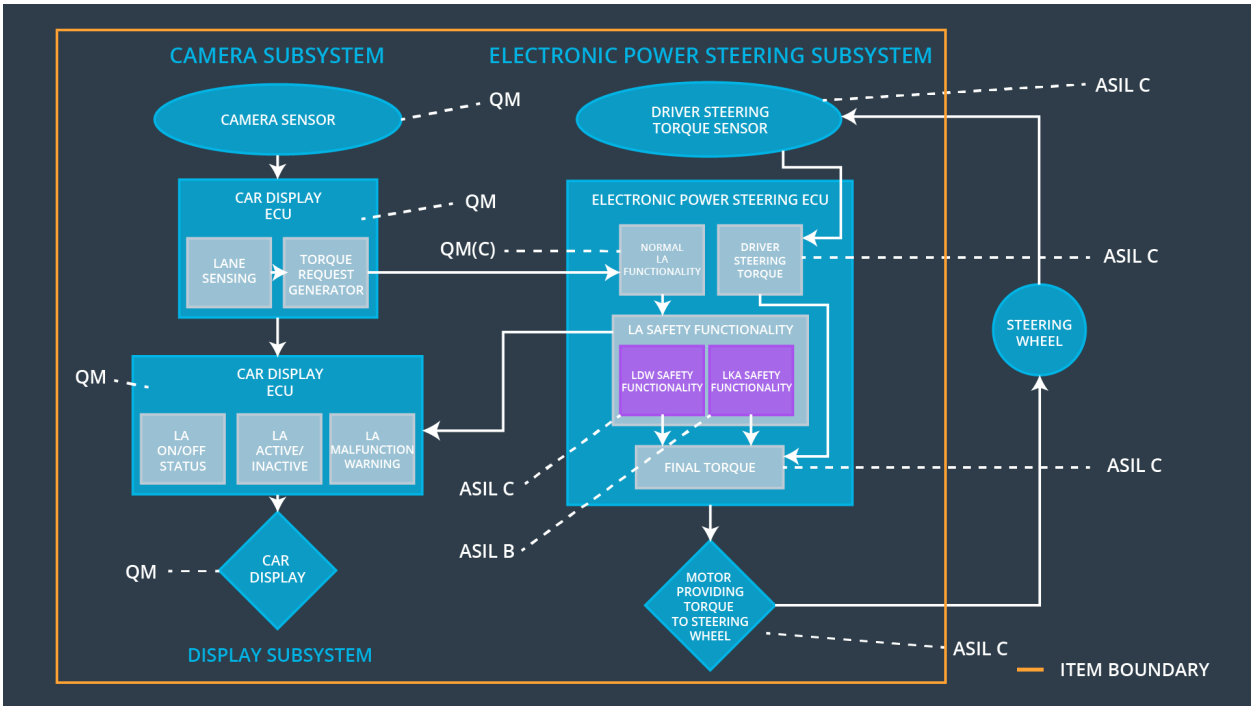
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	the electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	The lane keeping assistance torque is not applied

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	Making sure the max_duration chosen actually dissuade drivers from taking their hands off the wheel	Make sure the LKA system turns off when it is running 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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below max_torque_amplitude	**X**		
Functional Safety Requirement	The electronic power steering ECU shall ensure that the lane	**X**		

01-02	departure oscillating torque frequency is below max_torque_frequency			
Functional Safety Requirement 02-01	the electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	**X**		

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	The oscillation amplitude or frequency is greater than the maximum value allowed	Yes	A warning message will be flashed on car display showing that lane departure warning system is malfunctioning
WDC-02	Turn off the functionality	The LKA torque is applied for more than the maximum time allowed	Yes	A warning message will be flashed on car display showing that LKA is applied for too long, which will prompt the drivers to hold the steering wheel drive manually