



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
8/20/17	V1.0	Kris Harikrishnan	Initial document
8/25/2017	V1.1	Kris Harikrishnan	Revisions
8/26/2017	V1.2	Kris Harikrishnan	Incorporated feedback from Udacity reviewer

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]

[Document history](#)

[Table of Contents](#)

[Purpose of the Functional Safety Concept](#)

[Inputs to the Functional Safety Analysis](#)

[Safety goals from the Hazard Analysis and Risk Assessment](#)

[Preliminary Architecture](#)

[Description of architecture elements](#)

[Functional Safety Concept](#)

[Functional Safety Analysis](#)

[Functional Safety Requirements](#)

[Refinement of the System Architecture](#)

[Allocation of Functional Safety Requirements to Architecture Elements](#)

[Warning and Degradation Concept](#)

Purpose of the Functional Safety Concept

[Instructions: Answer what is the purpose of a functional safety concept?]

The functional safety concept looks at the general functionality of the item. In functional safety concept, we need to identify new requirements and allocate these requirements to system diagrams or system architecture.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

[Instructions:

REQUIRED:

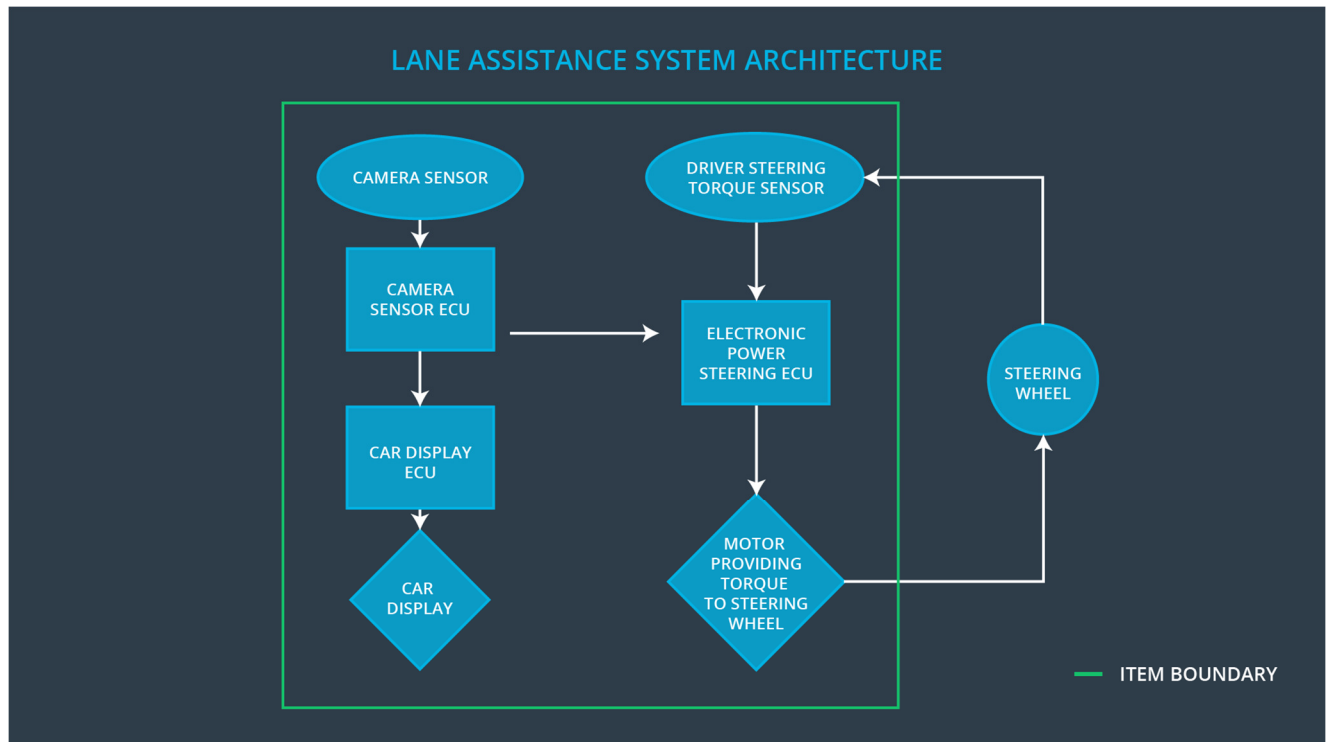
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

LDW Safety Goal: The oscillating steering torque from the lane departure warning function shall be limited.

LKA Safety Goal: The lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer 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	Takes lane pictures
Camera Sensor ECU	The camera ECU system detects lane departures through deep learning and computer vision techniques and tells the steering wheel ECU system how hard to turn as well as communicates with car display ECU to display the warning information
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
--	--	--	-----------------------------

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 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 Requirement 01-01	Test how drivers react to different torque amplitudes to prove that we chose an appropriate value	Verify that the safety requirement is met when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms 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 50 ms fault tolerant time interval

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

Lane Keeping Assistance (LKA) Requirements:

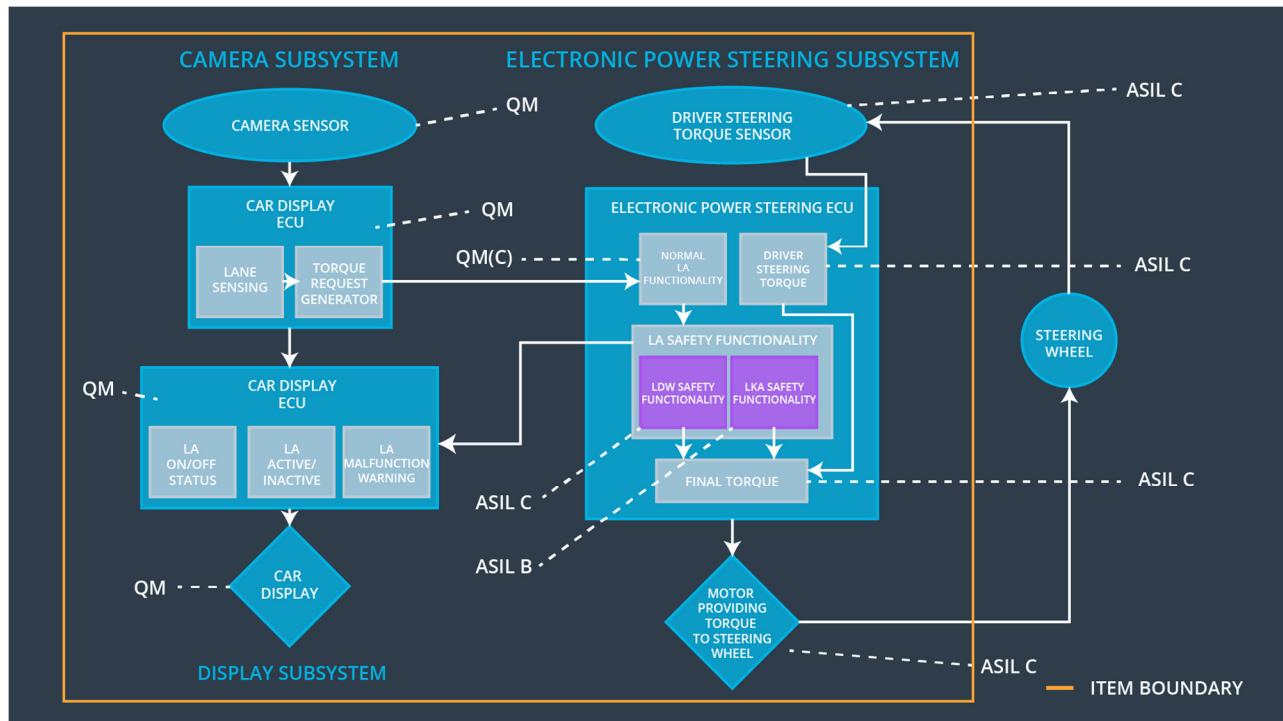
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	Shut off the system

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

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	X		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		
Functional Safety Requirement	The lane keeping item shall ensure that the lane keeping	X		

02-01	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_Frequency	Yes	Car display
WDC-02	Turn off	Lane keeping assistance torque is applied for longer than Max_Duration	Yes	Car display