Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [1.1]

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
1/29/19	1.0	Dylan Brandtner	First Attempt
1/30/2019	1.1	Dylan Brandtner	Updates from review

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?]
To allocate safety goals to requirements within the item architecture. The functional safety concept looks at the general functionality of the item and does not go into technical details.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

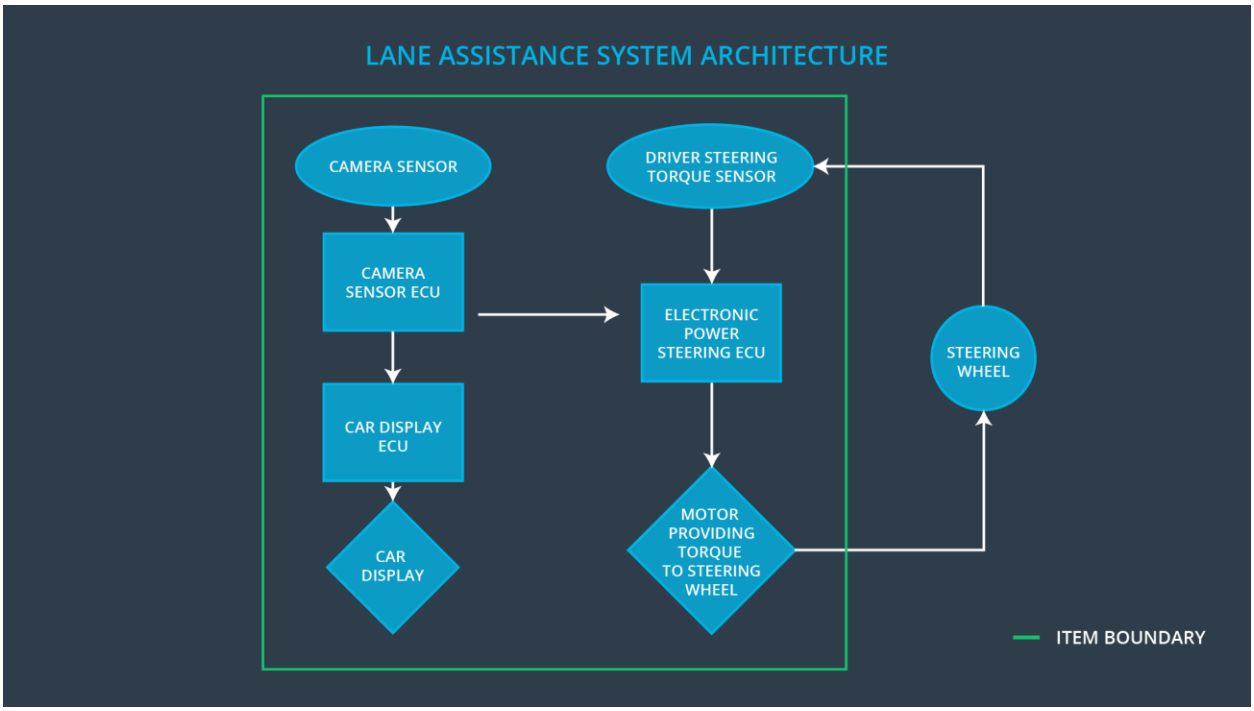
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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
Safety_Goal_03	The oscillating steering torque from the lane departure warning function shall be disabled during reverse

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	Reads in images from the road
Camera Sensor ECU	Identifies when the vehicle has departed lane and sends signal to Car display and Electronic Power Steering ECUs
Car Display	Displays information to the driver
Car Display ECU	Display lane departure warning to the driver
Driver Steering Torque Sensor	Identifies amount of steering torque currently being applied to wheels
Electronic Power Steering ECU	Determines the amount of steering torque to send to wheels to steer car back into ego lane
Motor	Provides steering torque to wheels

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
Malfunction_03	Lane Departure Warning (LDW) function shall apply an oscillating steering torque only when the vehicle is in Drive	WRONG	The lane departure warning function applies an oscillating torque in the wrong vehicle state

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	Torque 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	Torque set to 0
Functional Safety Requirement 01-03	The lane keeping item shall ensure that the lane departure oscillating torque is never applied while vehicle is not in Drive	QM	50ms	Torque 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	Validate Max_Torque_Amplitude is appropriate to avoid negative reaction to LDW	Verify oscillating torque never exceeds Max_Torque_Amplitude
Functional Safety Requirement 01-02	Validate Max_Torque_Frequency is appropriate to avoid negative reaction to LDW	Verify oscillating torque never exceeds Max_Torque_Frequency
Functional Safety Requirement 01-03	Validate drivers do not expect LDW to be active when vehicle is not in Drive	Verify oscillating torque is never applied when vehicle is not in drive.

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

Lane Keeping Assistance (LKA) Requirements:

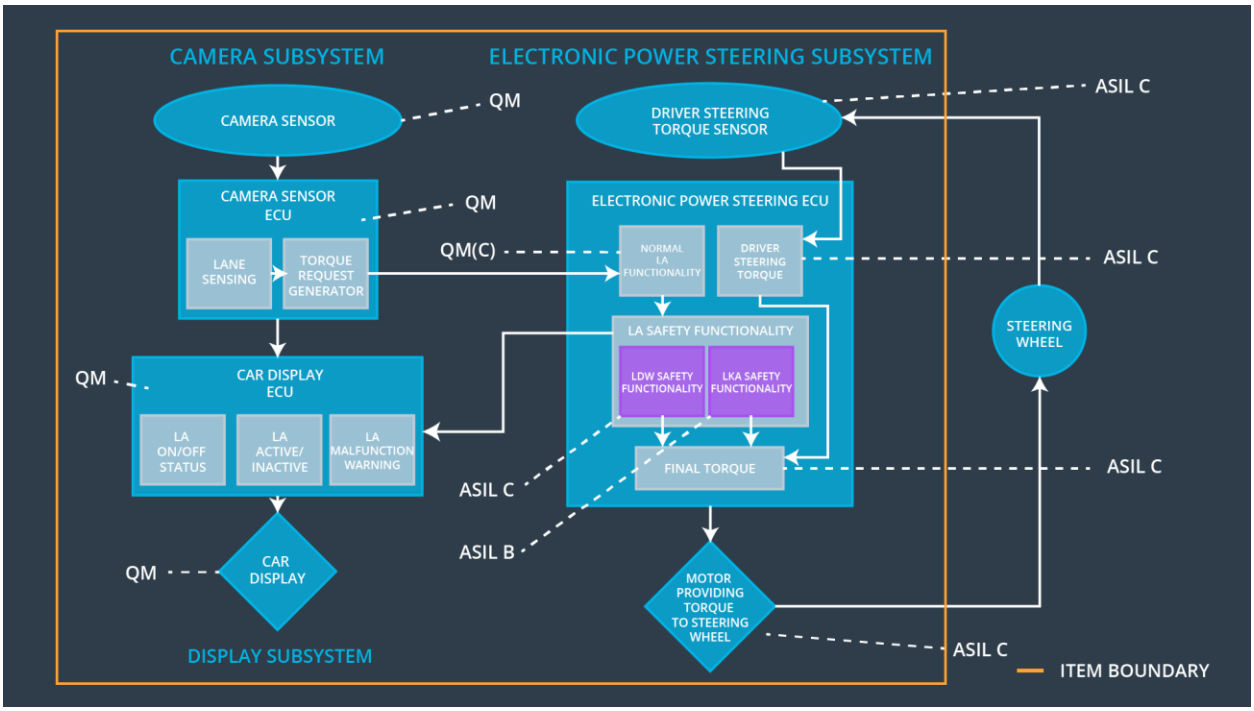
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	Electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500	Torque set to 0

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	Validate Max_Duration is appropriate to dissuade drivers from taking their hands off the wheel	Verify the LKA dues turn off if 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 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 01-03	The lane keeping item shall ensure that the lane departure oscillating torque is never applied while vehicle is not in Drive	**x**		
Functional Safety Requirement 02-01	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 LDW functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Warning light on Car Display shows user LDW is turned off
WDC-02	Turn of LKA functionality	Malfunction_03	Yes	Warning light on Car Display shows user LKA is turned off