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
2017-12-26	1.0	Sven Eriksson	Initial release
2017-12-26	2.0	Sven Eriksson	Updates to Verication and Validaction acceptance criteria to both LDW and LKA after feedback.

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?]

The purpose of the functional safety concept is to further analyze the item to identify new requirements and allocate these to system diagrams. The functional safety concept focuses on a high-level system description and the general functionality of the item.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

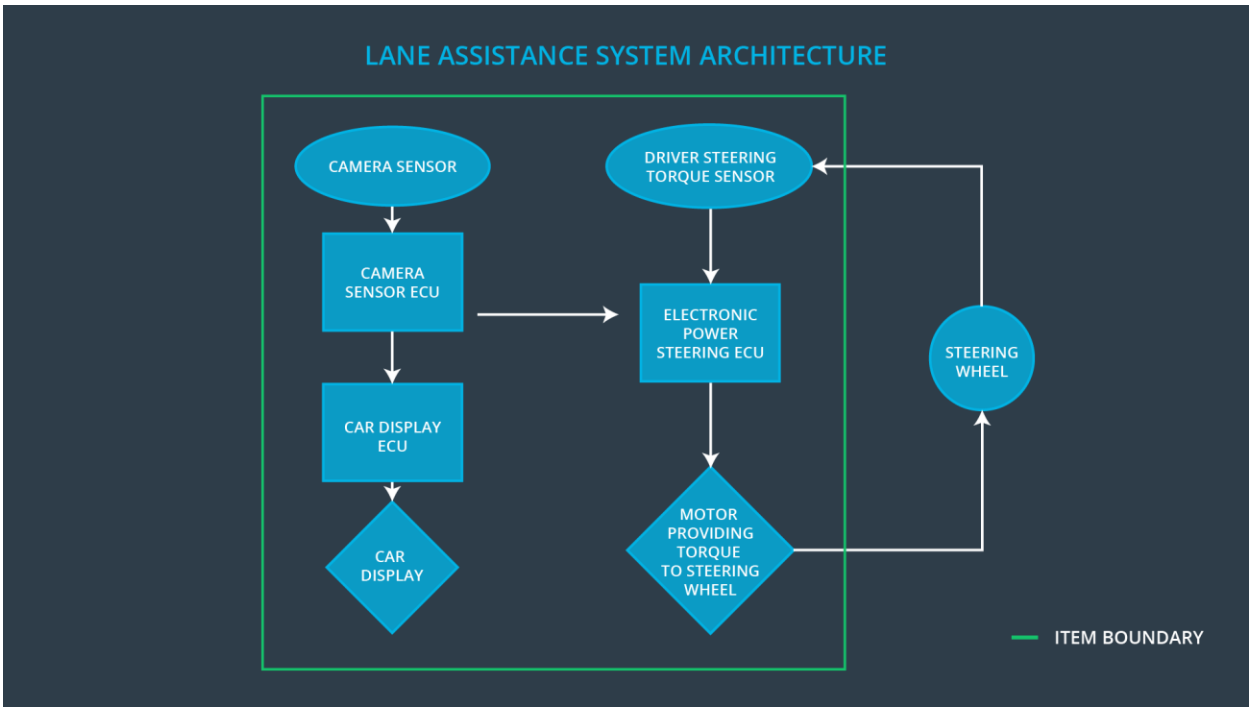
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 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	Captures an image of the road in front of the vehicle
Camera Sensor ECU	Processes that image
Car Display	Shows the state of the lane assistant item to the driver
Car Display ECU	Receives processed data from the Camera sensor ECU and prepares it to be shown to the driver
Driver Steering Torque Sensor	Measures the amount of torque the driver has applied
Electronic Power Steering ECU	Receives processed data from the Camera sensor ECU and controls the torque output
Motor	Applies 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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50mS	No torque is being applied to the steering wheel by the system.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50mS	No torque is being applied to the steering wheel by the system.

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	Criteria: Set a limit on the maximum torque amplitude allowed in the LDW functionality Method: Test how drivers react to different torque amplitudes.	Criteria: When torque amplitude crosses the limit, the lane assistance output is set to zero within the 50ms fault tolerant time interval. Method: Software test by inserting a fault into the system:
Functional Safety Requirement 01-02	Criteria: Set a limit on the maximum torque frequency allowed in the LDW functionality Method: Test how drivers react to different torque frequencies.	Criteria: When torque frequency crosses the limit, the lane assistance output is set to zero within the 50ms fault tolerant time interval. Method: Software test inserting a fault into the system

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

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	AS	Fault Tolerant	Safe State

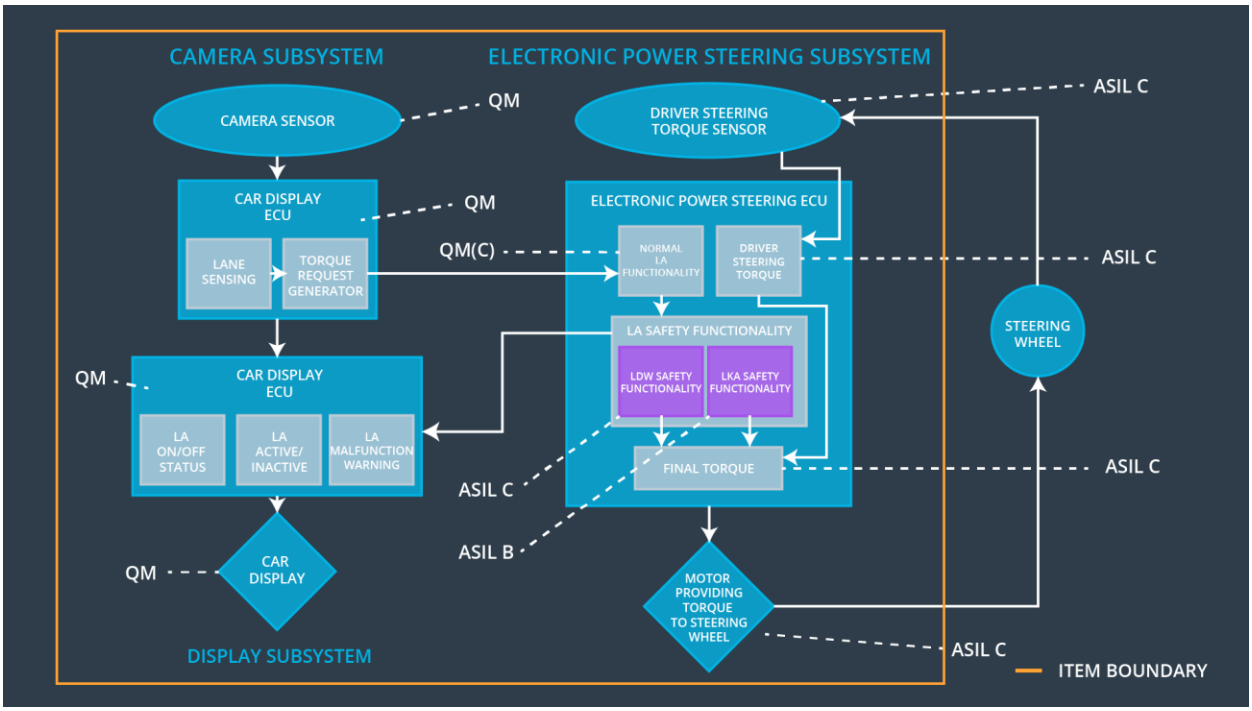
		I L	Time Interval	
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 mS	No torque is being applied to the steering wheel by the system.

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	Criteria: Set a time limit max_duration. Method: Test that the max_duration chosen really did dissuade drivers from taking their hands off the steering wheel.	Criteria: When the duration of applying torque from LKA exceeds max_duration, the lane assistance output is set to zero within the 500ms fault tolerant time interval. Method: In vehicle test with test driver.

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 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	**x**		
Functional	the electronic power steering	**x**		

Safety Requirement 02-01	ECU shall ensure that the lane keeping assistance torque is applied for only 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	The system will be turned off	Oscilating torque amplitude higher than Max_Torque_Amplitude	Yes	Warning light for LKA disabled on car display
WDC-02	The system will be turned off	Oscilating torque frequency higher than Max_Torque_Frequency	Yes	Warning light for LKA disabled on car display
WDC-03	The system will be turned off	Torque has been applied for more than Max_Duration	Yes	Warning light on the car display