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
25/5/2018	1.0	Mahmoud Taha	Initial document
26/5/2018	2.0	Mahmoud Taha	Resubmission

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?]
In Functional Safety Concept, safety goals are refined into safety requirements. These safety requirements are then allocated to the appropriate parts of the item's 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

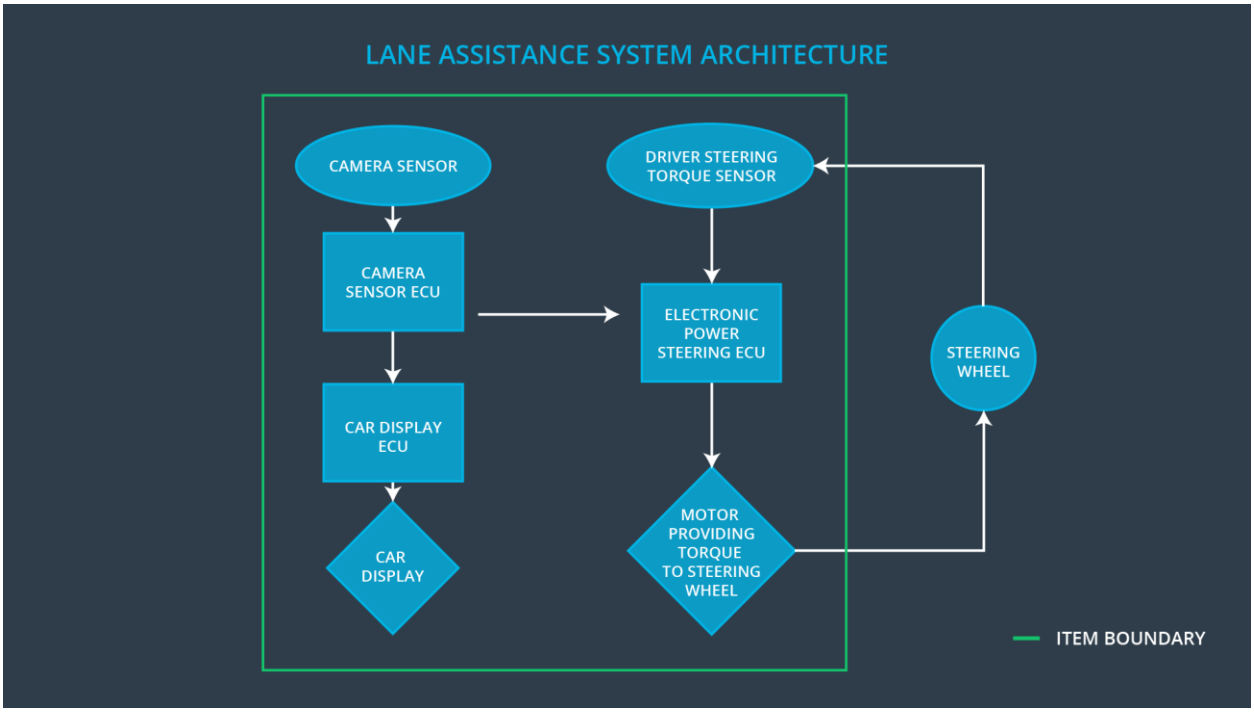
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 wheel from the LDW function shall be limited
Safety_Goal_02	The LKA function shall be time limited and the additional steering tourque shall end after a given amount of time interval so that the driver cannot misuse the system for

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	Input feed of the road and the environment
Camera Sensor ECU	Lane sensing Sending a torque request to the electronic power steering subsystem.
Car Display	Have display lights to tell the driver the status of different systems in the car
Car Display ECU	Controls the light that tells the driver if the lane keeping item is on or off Controls the light telling the driver that the lane departure warning is activated
Driver Steering Torque Sensor	Sense the driver steering torque
Electronic Power Steering ECU	Analyze driver steering torque Receive the vibrational torque request from the camera subsystem Add these torque requests together to output a final torque to the motor

Motor	Moves 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	deactivate the LDW feature and the toque shall be zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating frequency is below Max_Torque_Frequency	C	50ms	deactivate the LDW feature and the frequency shall be 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	The drivers reaction is safe when the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	The output is 0 torque amplitude within 50ms
Functional Safety Requirement 01-02	The drivers reaction is safe when the lane departure oscillating frequency is below Max_Torque_Frequency	The output is 0 torque frequency within 50ms

[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

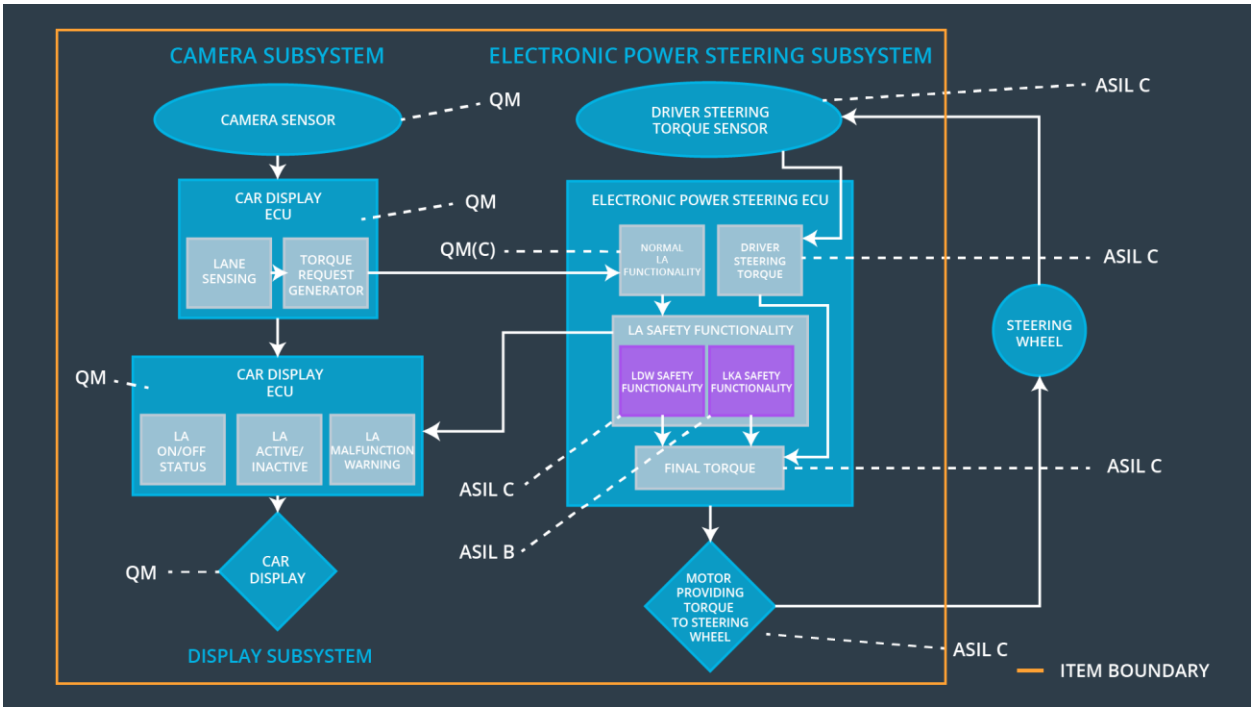
		I L	Time Interval	
Functional Safety Requirement 02-01	the electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	Turn off the LKA function and the torque shall be zero

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	The drivers reaction is safe when the lane keeping assistance torque is applied for only Max_Duration	The function is disabled within 500ms

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 frequency is below Max_Torque_Frequency	**x**		
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.]

Referring to "Functional Safety Analysis" above, Malfunctions 01,02 (LDW) become trigger modes for WDC-01 and Malfunctions 03 (LKA) for WDC-02.

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the functionality	the lane departure oscillating torque amplitude or frequency	Yes	A warning light will turn on

		exceeded their thresholds		
WDC-02	Turn off the LKA functionality	the lane keeping assistance torque is applied for more than Max_Duration	Yes	A warning light will turn on