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
01/05/19	1.0	C.Wong	Initial Version

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 ultimate goal of functional safety is to avoid accidents by reducing risks to acceptable levels. The functional safety concept looks at items from a higher level, the system architectural design, and identifies what items (item architecture) affect safety. Safety goals are developed for those items, which then functional safety requirements can be derived.

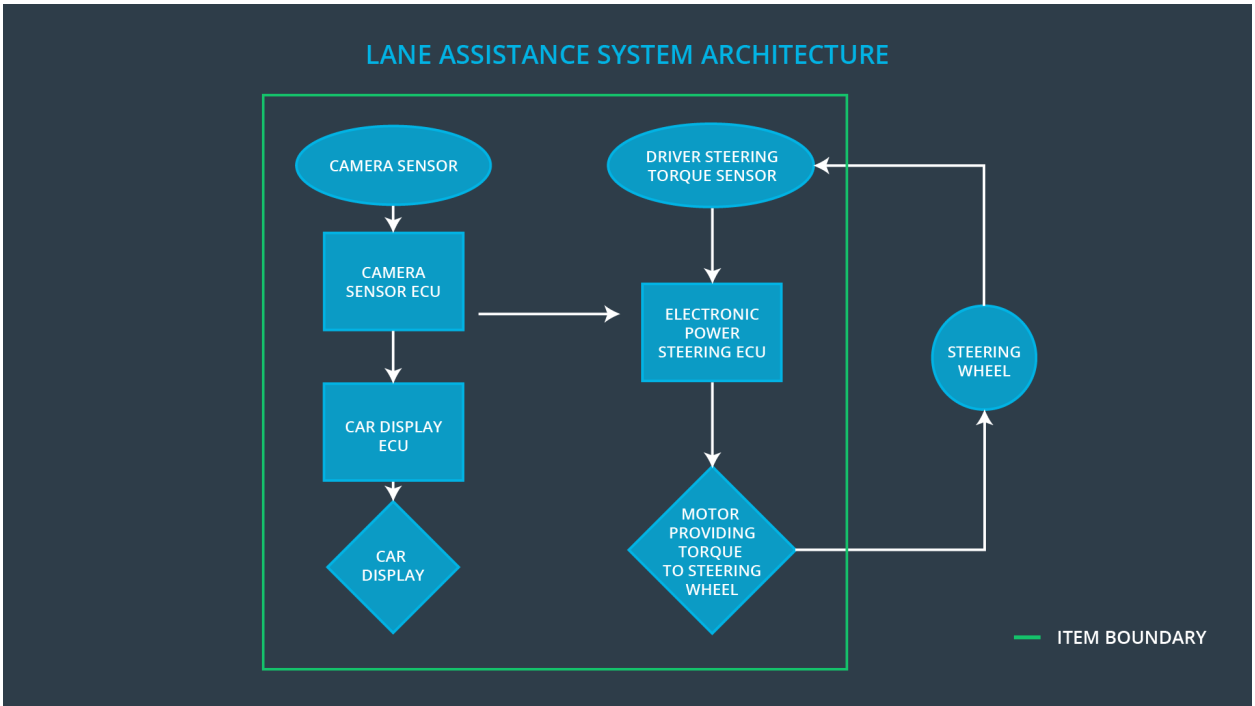
Inputs to the Functional Safety Concept

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 oscillation torque by the LDW (Lane departure warning) function shall be limited. (ASIL C)
Safety_Goal_02	The LKA (Lane keeping assistance) function shall limit steering torque to prevent sharp vehicle movements during rapid disengagement and engagement due to lane loss. (ASIL C)



Element	Description
Camera Sensor	Captures image and converts to pixel data sent to Camera Sensor ECU
Camera Sensor ECU	Receives pixel data from camera sensor, determines if vehicle is within target lane. A status of whether the car is in or out of a lane is sent to the Car Display ECU and Power Steering ECU
Car Display	Displays a warning or status when it receives car display ECU data.
Car Display ECU	Receives status camera sensor ecu status and updates car display
Driver Steering Torque Sensor	Measures the torque applied by the driver and sends to the driver sterring torque subsystem
Electronic Power Steering ECU	Receives camera sensor ecu status and driver steering torque sensor data, calculates the torque and time duration needed for provide a haptic output/vibration to the steering wheel.
Motor	Receives commands from the Electronic Power Steering ECU and 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	LDW function applies an oscillating steering torque that is above limit, i.e. too much
Malfunction_02	Lane Departure Warning (**LDW**) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	LDW function applies an oscillating steering torque that is unexpected.
Malfunction_03	Lane Keeping Assistance (**LKA**) function shall apply the steering torque when active in order to stay in ego lane	NO	LKA function disengages because camera ECU does not detect lane due to camera sensor intermittently seeing lane due to fog.
Malfunction_04	Lane Keeping Assistance (**LKA**) function shall apply the steering torque when active in order to stay in ego lane	WRONG	LKA function engages while driving backwards because the forward camera detects a lane and corrects for it.

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	(**LDW**) The electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Off
Functional	(**LDW**) The electronic power steering ECU	C	50 ms	Off

Safety Requirement 01-02	shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency			

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	Define a reasonable limit for Max_Torque_Amplitude for LDW.	When the torque amplitude crosses the defined limit, system is turned off within the 50ms
Functional Safety Requirement 01-02	Define a reasonable limit for Max_Torque_Frequency for LDW.	When the torque frequency crosses the defined limit, system is turned off within the 50ms

[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 LKA torque is applied for only Max_Duration	C	500 ms	Off
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the LKA torque is always zero while the vehicle is in reverse (moving backwards)	B	500 ms	Off

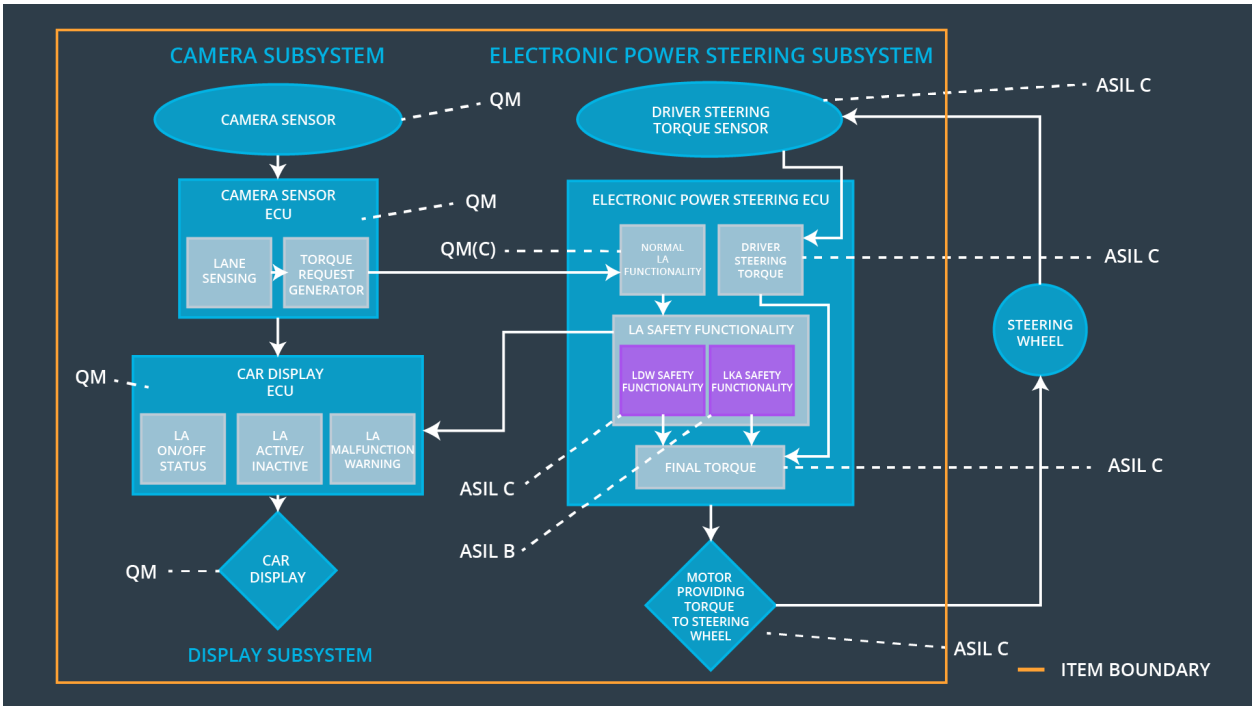
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method

Functional Safety Requirement 02-01	Set the reasonable value of Max_Duration.	Verify that the system turns off if the LKA exceeds the Max_Duration.
Functional Safety Requirement 02-02	Set Reverse_Mode_Torque to TRUE.	Verify the system turns off if the LKA mode flag Reverse_Mode_Torque is set to TRUE

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	Camera ECU	Car Display ECU

		Steering ECU		
Functional Safety Requirement 01-01	Electronic Power Steering ECU shall ensure that the lane departure torque amplitude shall not exceed Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	Electronic Power Steering ECU shall ensure that the lane departure torque frequency shall not exceed Max_Torque_Frequency.	**X**		
Functional Safety Requirement 02-01	Electronic Power Steering ECU shall ensure that the LKA torque application is time limited for only Max_Duration,	**X**		
Functional Safety Requirement 02-02	Electronic Power Steering ECU shall ensure that the LKA torque application is turned off if Reverse_Mode_Torque is TRUE	**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	Off	If LDW Torque oscillation amplitude exceeds Max_Torque_Amplitude OR Torque oscillation frequency exceeds Max_Torque_Frequency	Yes	Warning light on the Car Display

WDC-02	Off	If LKA torque applied for the duration longer than the Max_Duration	Yes	Warning light on the Car Display
WDC-03	Off	If vehicle transmission set to reverse, then Reverse_Mode_ Torque is TRUE	Yes	Warning light on the Car Display