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
28-Oct-2017	1.0	R Hariharan	Functional Safety Concept for Lane Assistance Step by Step

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?]

- A functional safety concept generates functional safety requirements from the general functional safety goals. These requirements are allocated to subsystems and parts of the system.
- The system architecture may require modification to meet the functional safety requirements.
- The functional safety concept reviews general functionality of an item but does not include the technical implementation of the design.
- Information in the functional safety analysis comes from the hazard analysis and risk assessment.
- Functional Safety requirements also have a few attributes that need to be specified in the functional safety concept:
  - the ASIL level
  - the fault tolerant time interval, which measures how quickly a system needs to react to a hazardous situation
  - And the safe state, which discusses what a system looks like after it has avoided an accident.

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.

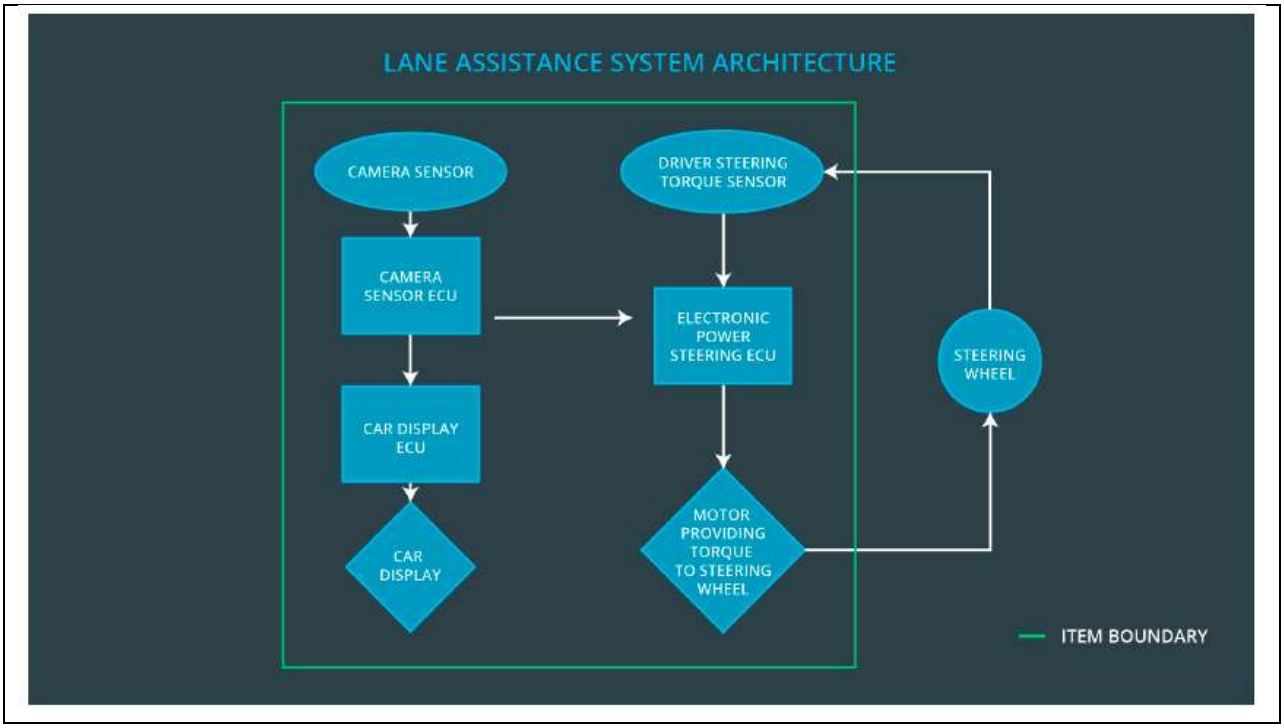
OPTIONAL:
If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.
]

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the LDW (Lane Departure Warning) function shall be limited
Safety_Goal_02	The LKA (Lane Keeping Assistance) function shall be time limited and the additional steering torque shall end after a given time interval

Safety_Goal_03	The LKA function shall be deactivated during snowfall (degraded view) conditions
Safety_Goal_04	The LKA function shall be deactivated during heavy steering input by the driver

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	Generally mounted on the Front side of the Vehicle, it captures and sends an image stream to the Camera Sensor ECU
Camera Sensor ECU	It is an electronics hardware and processor or micro-controller responsible for interpreting the received data from camera sensor, to identify lane markings and determine the vehicle position and issuing appropriate torque requests to the electronic power steering ECU
Car Display	Vehicle dashboard lights or display / screen unit providing status feedback to the driver of vehicle systems.
Car Display ECU	Takes the input from camera sensor ECU and controls the logic to display the warning (LED lights) in car display if LDW or LKW are detected.
Driver Steering Torque Sensor	Physical sensor capable of measuring steering torque input on the steering wheel from the driver.
Electronic Power Steering ECU	Takes input from camera ECU and driver steering torque sensor and calculates the necessary torque needed as well as time duration for LKA.
Motor	The motor which applies torque to the steering column, accepts voltage / current control from the Power Steering ECU.

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	LKA 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	Turn off LDW
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	Turn off LDW

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.	Software testing is used to command a torque larger than Max_Torque_Amplitude: 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.	Software test: When the torque frequency crosses the limit of Max_Torque_Frequency, 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:

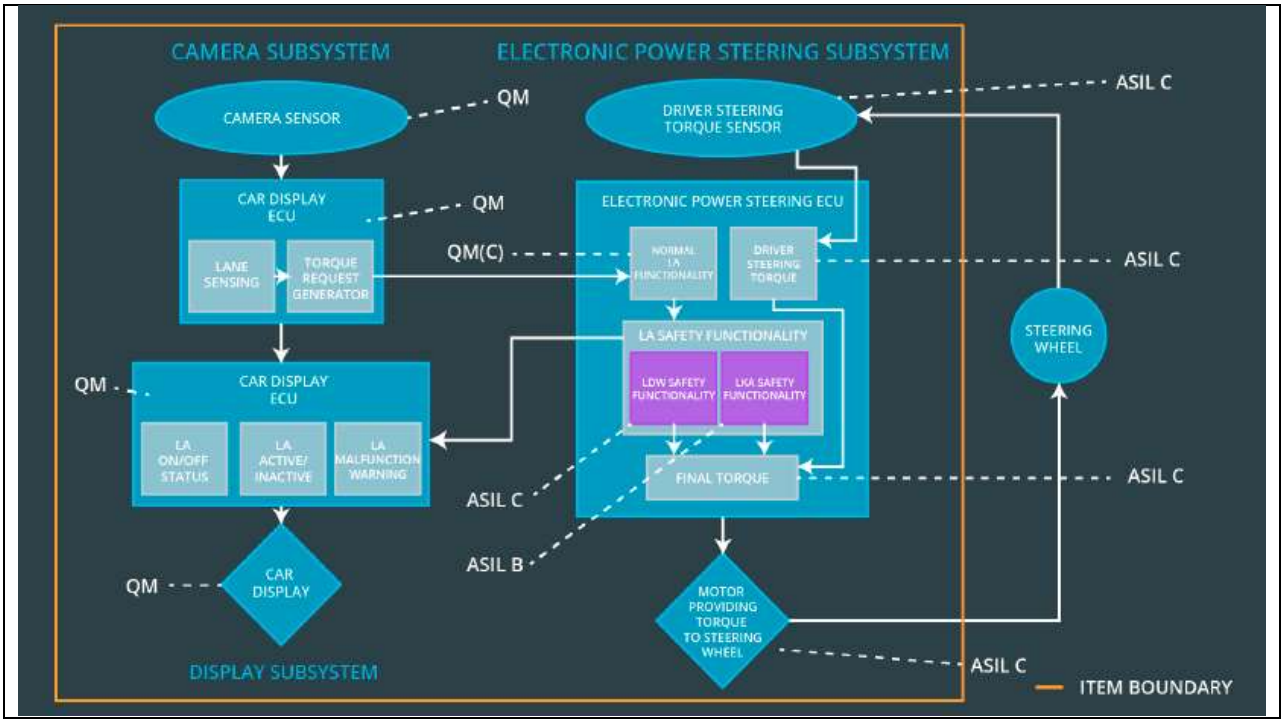
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	turn off functionality

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	Define a reasonable limit for Max_Duration. Test and validate the chosen value resulted in dissuading the drivers from taking their hands off the wheel.	Verify the system turn off the LKA after 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	Test how drivers react to different torque amplitudes to prove that we chose an appropriate value.	**X**		
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that we chose an appropriate value.	**X**		
Functional Safety Requirement 02-01	Define a reasonable limit for Max_Duration. Test and validate the chosen value resulted in dissuading the drivers from taking their hands off the x`wheel.	**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 Torque amplitude exceeds Max_Torque_Amplitude or Torque frequency exceeds Max_Torque_Frequency	YES	Warning light in car display
WDC-02	OFF	If LKA torque applied exceeds the Max_Duration time interval	YES	Warning light in car display