Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [1.0]

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
24 June 2019	1.0	Guilin Zhu	First version for functional safety concept
26 June 2019	1.1	Guilin Zhu	Updated FTTI for LKA req to 500ms

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 functional safety concept is to derive higher level functional safety requirements from safety goals, which are derived from hazard analysis and risk assessment as well as refine the system architecture.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

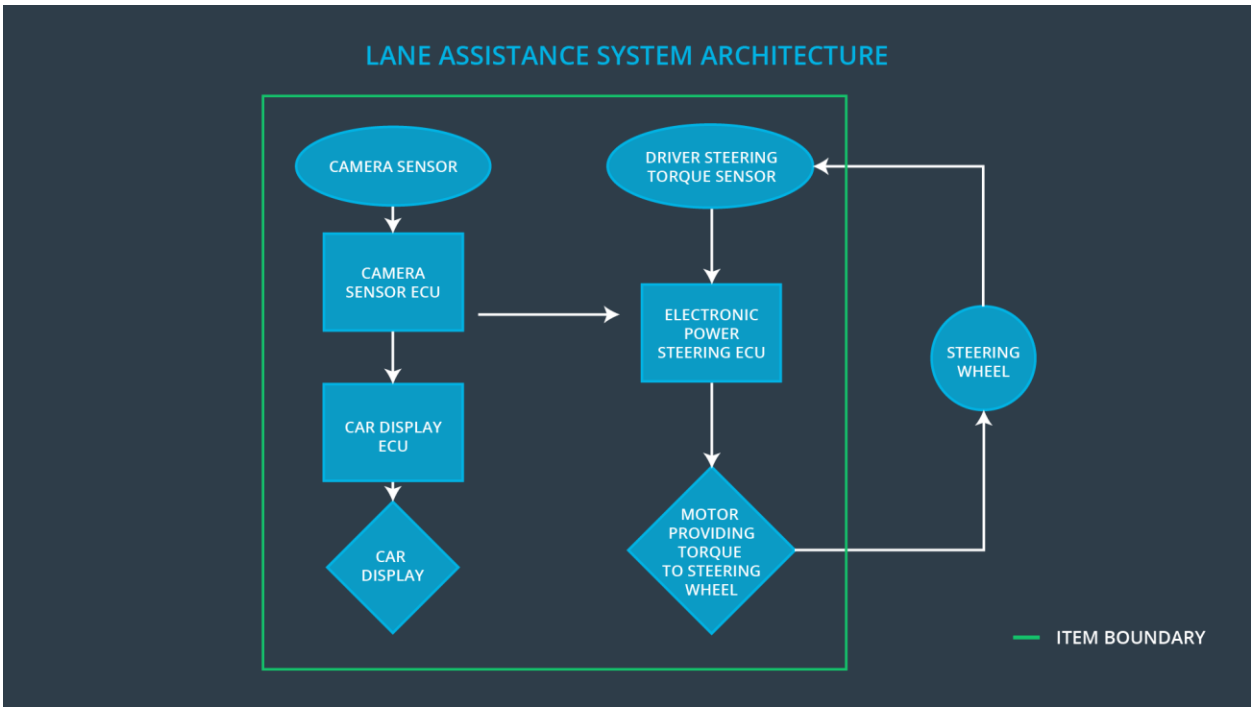
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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

ID	Safety Goal
Safety_Goal_01	Unintended oscillating torque shall be prevented/limited for LDW function
Safety_Goal_02	LKA function shall detect/report driver hands off the wheel within certain amount of time
Safety_Goal_03	LKA function shall keep in ego lane and unintended torque command shall be prevented

Preliminary Architecture

[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]
The current lane assistance system architecture is shown below:



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	Responsible for detecting lane lines
Camera Sensor ECU	Responsible for determining when vehicle leaves the lane by mistake
Car Display	Responsible for displaying warning as to whether the vehicle is leaving the lane
Car Display ECU	Responsible for determining the warning coming from lane departure warning function
Driver Steering Torque Sensor	Detect driver's intention/torque on the steering wheel
Electronic Power Steering ECU	Responsible for determining/calculating an appropriate amount of torque based on lane assistance system torque request
Motor	Responsible for providing the torque command from EPS 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	Lane departure warning (LDW) function applies an oscillating steering torque above the 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	Lane keeping assistance function has no hands on the steering wheel.
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	More	Lane Keeping Assistance (LKA) function applies more torque command than expected when active

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 EPS shall ensure the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Lane assistance output ramp out to zero and disable LDW
Functional Safety Requirement 01-02	The EPS shall ensure that lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Lane assistance output ramp out to zero and disable 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	The driver is able to control the vehicle when Max_Torque_Amplitude is set to different values	When fault is injected into torque amplitude signal and it exceeds the limit, the lane assistance output is set to zero within 50ms
Functional Safety Requirement 01-02	The driver is able to control the vehicle when Max_Torque_Frequency is set to different values	When fault is injected into torque frequency signal and it exceeds the limit, the lane assistance output is set to zero within 50ms

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

Lane Keeping Assistance (LKA) Requirements:

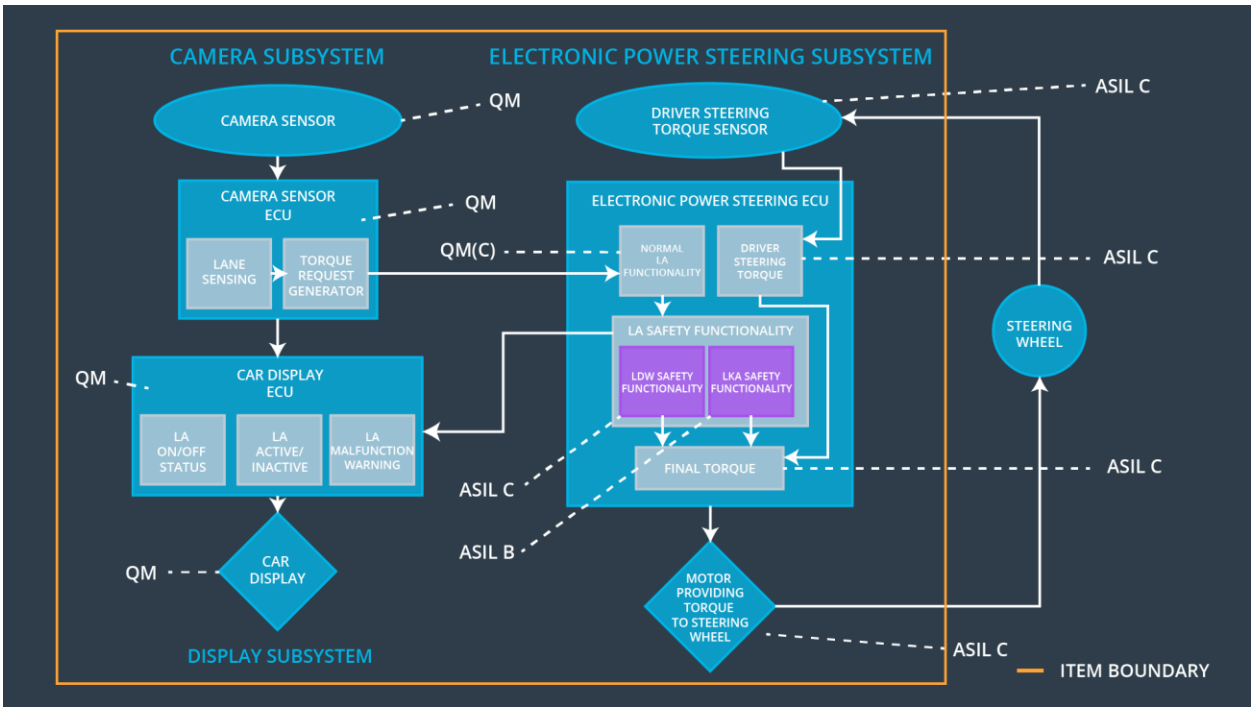
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The EPS shall ensure that LKA function is able to detect driver hands off the wheel for Max_duration	B	500ms	System warning and LKA ramp out torque command, disable LKA
Functional Safety Requirement 02-02	The EPS shall ensure that LKA function torque output is below Max_Cmd	B	500ms	System warning and LKA ramp out torque command, disable LKA

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 Max_duration is chosen/tested in the vehicle	When driver's hands off the steering wheel for more than Max_duration, the LKA function ramp out and disble the output.

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 electric power steering ECU shall ensure the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	**x**		**x**
Functional Safety	The electric power steering ECU shall ensure that lane departure	**x**		**x**

Requirement 01-02	oscillating torque frequency is below Max_Torque_Frequency			
Functional Safety Requirement 02-01	The electric power steering subsystem shall ensure that LKA function is able to detect driver hands off the wheel for Max_duration	**x**		**x**
Functional Safety Requirement 02-02	The EPS shall ensure that LKA function torque output is below Max_Cmd	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	LDW function off	When the oscillating torque above the limit	Yes	The driver will be alerted by the Car display
WDC-02	LKA function off	When driver's hands off the steering wheel for more than Max_duration	Yes	The driver will be alerted by the Car display