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
August 13,2017	1.0	Ryosuke Honda	Initial Draft
August 14,2017	2.0	Ryosuke Honda	Revised Functional Safety Requirements and add "Refinement of System Architecture" diagram.

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]

Document history

Table of Contents

Purpose of the Functional Safety Concept

Inputs to the Functional Safety Analysis
- Safety goals from the Hazard Analysis and Risk Assessment
- Preliminary Architecture
  - Description of architecture elements

Functional Safety Concept
- Functional Safety Analysis
- Functional Safety Requirements
- Refinement of the System Architecture
- Allocation of Functional Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Functional Safety Concept

[Instructions: Answer what is the purpose of a functional safety concept?]

There are three purposes of the Functional Safety Concept.

- Refine the safety goals in what are called safety requirements.
- Allocate these safety requirements to the relevant parts of the system diagram.
- Refine the system architecture.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

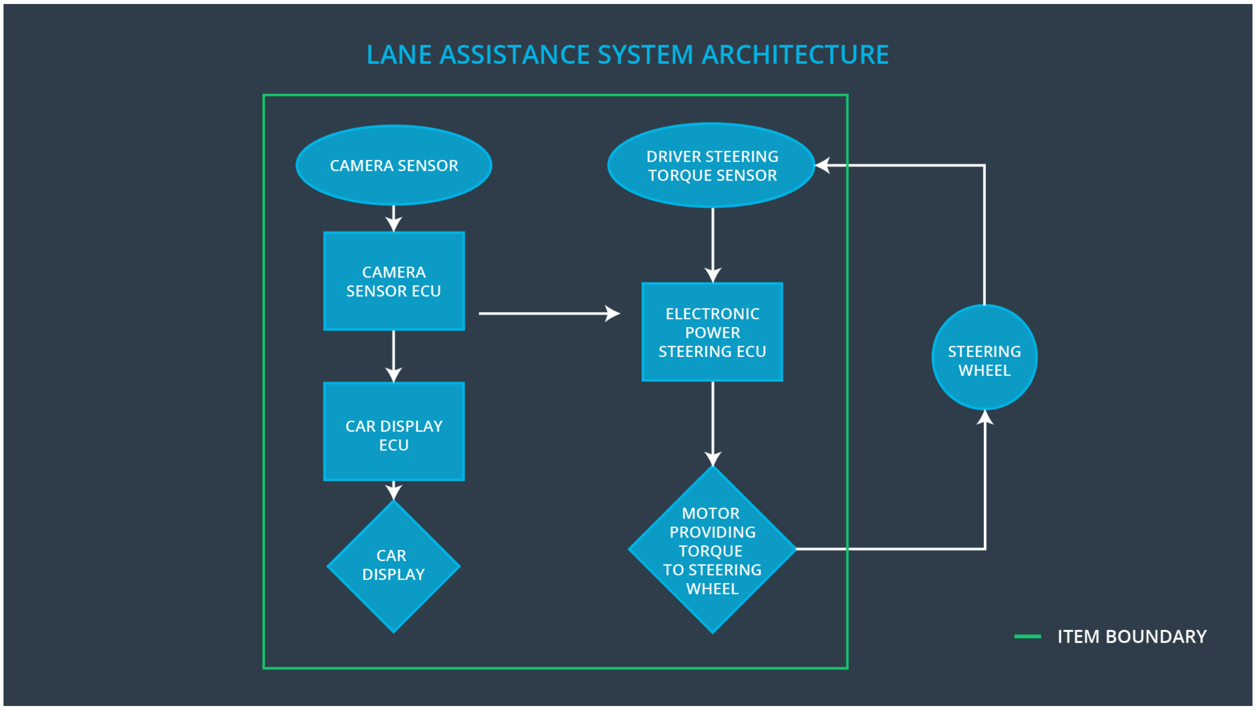
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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

ID	**Safety Goal**
Safety_Goal_01	The oscillating sttering torque from the lane departure warning function shall be limited.
Safety_Goal_02	The lane keeping assistance torque is applied only limited time duration.
Safety_Goal_03	The use of camera in degraded view condition shall be limited.

Preliminary Architecture

[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

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	Camera sensor is responsible for capturing the vehicle driving condition including detactable lane lines.
Camera Sensor ECU	Camera Sensor ECU is responsible for measuring the distance from the lane line and making requests how much torque to generate to Electronic Power Steering ECU.
Car Display	Car Display is responsible for warning the driver of misuse of lane keeping system or letting the driver know of the lane departure or lane keeping system malfunction.
Car Display ECU	Car Display ECU is responsible for recieving the distance information from the Camera Sensor ECU and deciding whether or not send a warn signal to the

	Car DIsplay.
Driver Steering Torque Sensor	Driver Steering Torque Sensor is responsible for measureing driver steering torque.
Electronic Power Steering ECU	Electronic Power Steering ECU is responsible for recieving steering torque from Driver Steering Torque Sensor and the torque request from Camera Sensor ECU and then finalize the steering torque request to Motor.
Motor	Motor is responsible to provide torque to 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	MORE	The lane departure warning function applies an oscillating torque with very high torque

	driver a haptic feedback		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	Set vibration torque to zero
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequecy.	C	50ms	Set vibration torque to 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 Max_Torque_Amplitude is large enough to let drivers know the haptic feedback.	Verify that the amount of oscillating torque amplitude is below Max_Torque_Amplitude

Functional Safety Requirement 01-02	The Max_Torque_Frequency is large enough to let drivers know the haptic feedback.	Verify that the amount of oscillating torque freqency is below Max_Torque_Freqency.

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

Lane Keeping Assistance (LKA) Requirements:

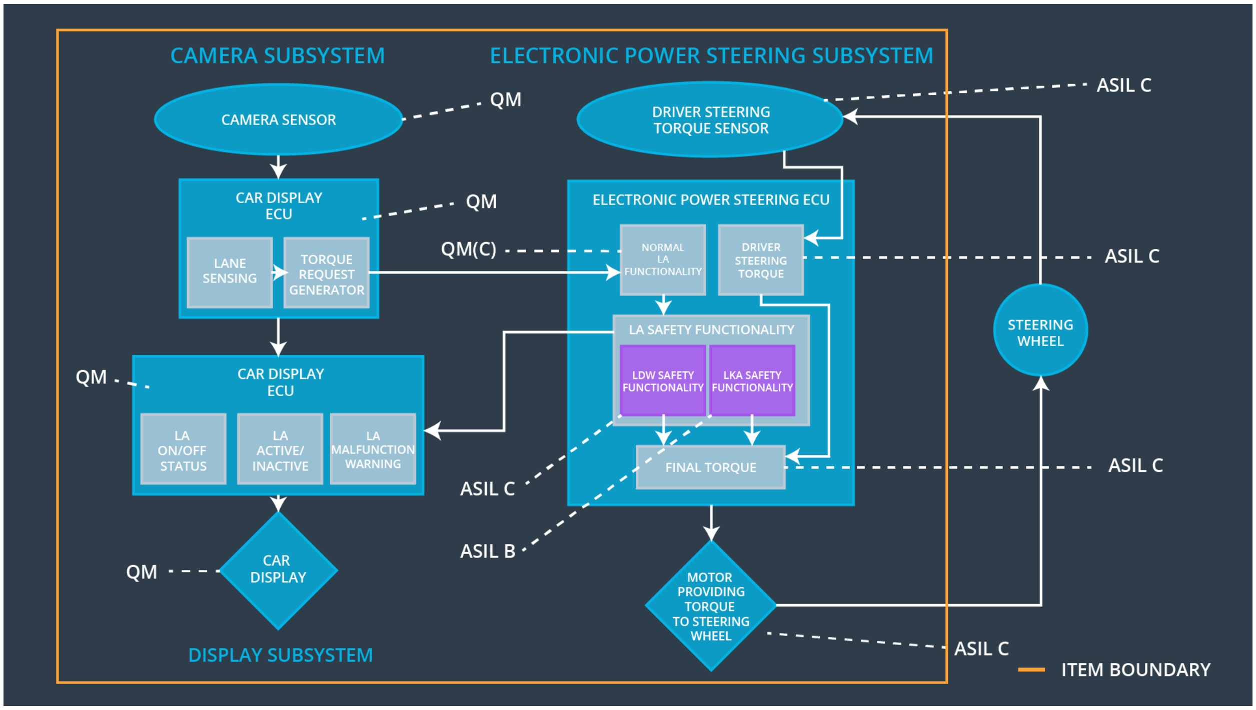
ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500ms	Shut off the system

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	The Max_Duration chosen really did dissuade drivers from taking their hands off the wheel.	The system really does turn off if the lane keeping assistance every exceeded Max_Duration.

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_Frequecy.	X		
Functional	The lane keeping item shall	X		

Safety Requirement 02-01	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	Trun off the functionality	Maximum torque is beyond Max_Torque_Amplitude	Yes	Car Display
WDC-02	Trun off the functionality	Maximum torque is beyond Max_Torque_Freqency	Yes	Car Display
WDC-03	Trun off the functionality	Maximum duration is beyond Max_Duration	Yes	Car Display