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
2018-12-01	1.0	Flash Yuan	First draft of the Functional Safety Concept for Lane Assistance

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?]

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

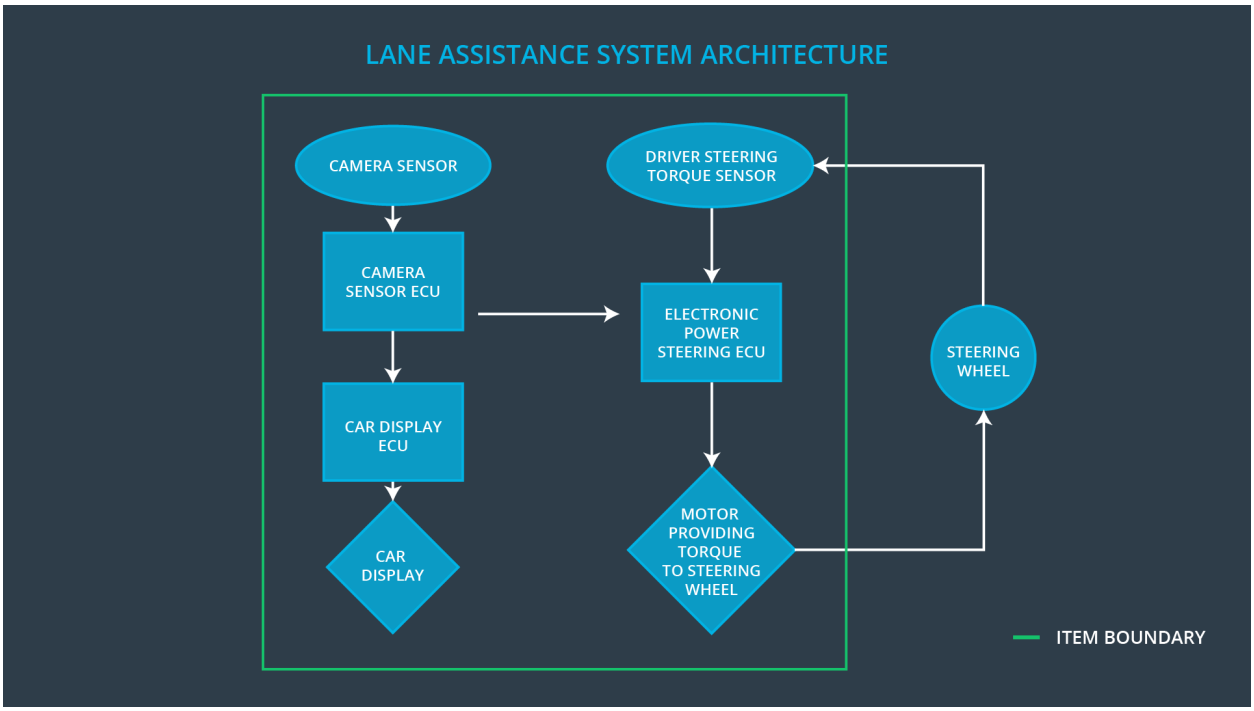
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 lane departure warning function shall be limited
Safety_Goal_02	The lane keeping assistance function shall be time limited, and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.

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	Reads the images and sends to camera sensor ECU
Camera Sensor ECU	Receives images from the camera and identifies when vehicle has departed the lanes by mistake and sends the message to the Car Display ECU and electronic power steering ECU.
Car Display	Displays if car has departed the lane by mistake
Car Display ECU	Receives input from the camera sensor ECU and updates the Car Display to show the information
Driver Steering Torque Sensor	Measures the torque applied by the driver
Electronic Power Steering ECU	Receives input from the camera Sensor ECU and driver steering torque sensor and **calculates** the torque and time duration needed for LKA and **update** the motor.
Motor	Takes input from the Electronic Power Steering ECU and provides the 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 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	LDW 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	50 ms	Off (oscillating torque is 0 and hence no torque is applied to the steering wheel)
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Off

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	A	Fault	Safe State

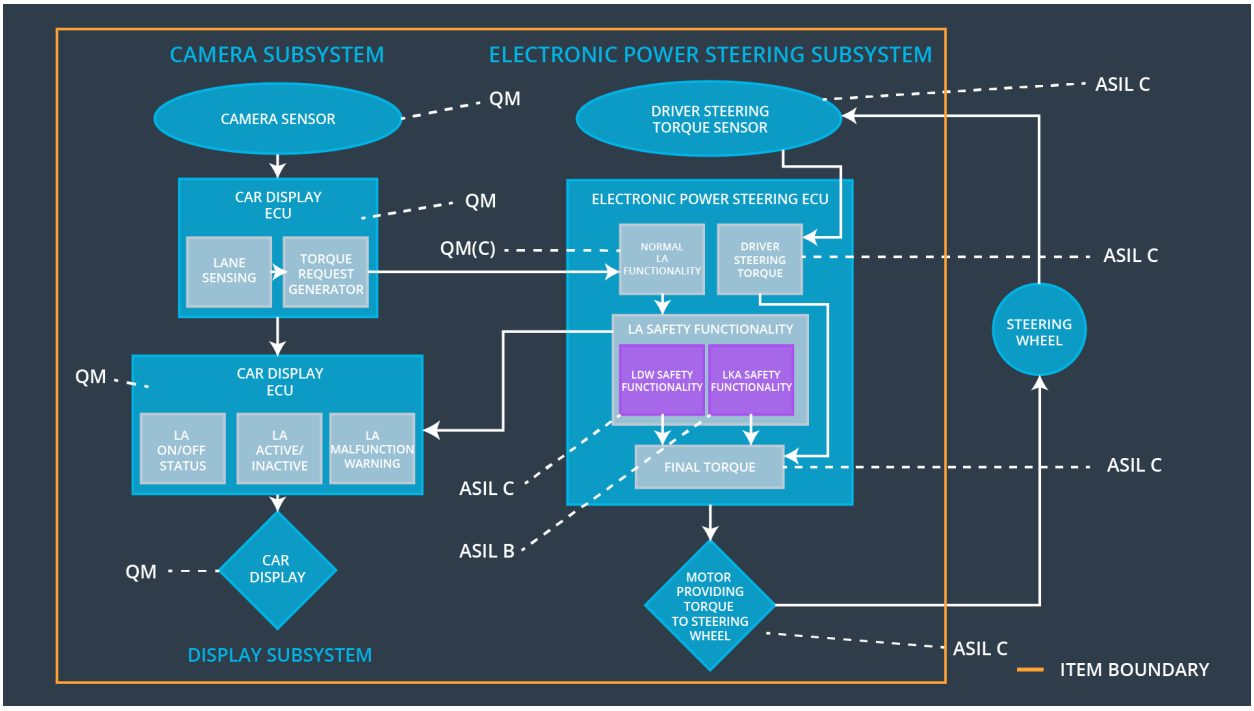
		SIL	Tolerant Time Interval	
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the LKA torque is applied for only Max_Duration	B	500 ms	Off

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. Validate that the chosen value resulted in **dissuading** the drivers from taking their hands off the wheel	Verify that the system turns off if the LKA exceeds the 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	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**		

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 oscillation amplitude exceeds Max_Torque_Am	Yes	Warning light on the Car Display

		plitude OR Torque oscillation frequency exceeds Max_Torque_Frequency		
WDC-02	Off	If torque applied for the duration longer than the Max_Duration	Yes	Warning light on the Car Display