Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: v1.1

Version 1.1, Released on 2018-06-25

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
6/25/2018	V1.1	Aaron Li	1st submission

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?]
Avoid accidents by reducing risk to acceptable levels.

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	lane departure warning
Safety_Goal_02	lane keeping assistance

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	Take in the image from environment; send it to camera sensor ECU

Camera Sensor ECU	Take in the image from camera sensor; process in the information and send instruction to car display ECU and electronic power steering ECU
Car Display	Take information from car display ECU, display to driver
Car Display ECU	Take in the data from camera ECU; send information to car display
Driver Steering Torque Sensor	Sensing the torque generated from motor, and send it to electronic power steering ECU
Electronic Power Steering ECU	Take information from camera sensor ECU and drive steering torque ECU, compute the right torque to actuator, send it to motor
Motor	Take information from electronic power steering ECU, generate torque

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	Less	Driver failed to catch the haptic signal to trigger corrective action

Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	More	Driver loss control over the steering wheel
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	More	Driver loss focus and abuse the function; less response to emergency situation, and leads to crash

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 shall has a lower limit so that the driver can capture the haptic signal, and not miss the notification.	B	500ms	Driver will notice when the car is off the lane
Functional Safety Requirement 01-02	LDW shall has a upper limit so that the driver can still get control over the steering wheel when the haptic is on.	D	500ms	Driver will get back control when the LDW haptic is 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	We would need to test how drivers react to different torque amplitudes and frequencies to prove that we chose an appropriate value.	when the torque amplitude crosses the **lower** limit, the lane assistance output is set to lower limit within the 50 ms fault tolerant time interval.
Functional Safety Requirement 01-02	We would need to test how drivers react to different torque amplitudes and frequencies to prove that we chose an appropriate value.	when the torque amplitude crosses the **upper** limit, 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	LKA shall have a upper limit, so that driver will not lose focus, or abuse the system.	D	500ms	Driver will have a delay in reaction to emergent situations.

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	We would need to test how long it would take for the drivers to lose focus when the car is keeping in lane itself.	when the time duration crosses the limit, the lane assistance will turn off so that to catch the driver's attention back, preventing abuse of the system.

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	LDW shall has a lower limit so that the driver can capture the haptic signal, and not miss the notification.	X		
Functional Safety Requirement 01-02	LDW shall has a upper limit so that the driver can still get control over the steering wheel when the haptic is on.	X		
Functional Safety Requirement 02-01	LKA shall have a upper limit, so that driver will not lose focus, or abuse the system.	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 haptic loose control	Haptic go beyond upper limit	yes	Lights up on the dashboard
WDC-02	LDW haptic loose control	Haptic go below lower limit	yes	Lights up on the dashboard