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
04/26/2019	1.0	Chuan Yu	Update inputs to functional safety analysis
04/27/2019	2.0	Chuan Yu	Update functional safety concept

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 purposes of the functional safety concept are:

1. Figure out what subsystems actually contain high levels of risk and what's needed to prevent accidents
2. Figure out which subsystems and elements can be used to meet safety goals
3. Further refine above high level goals into functional safety requirements
4. Allocate each functional safety requirement to its appropriate place in the item architecture

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

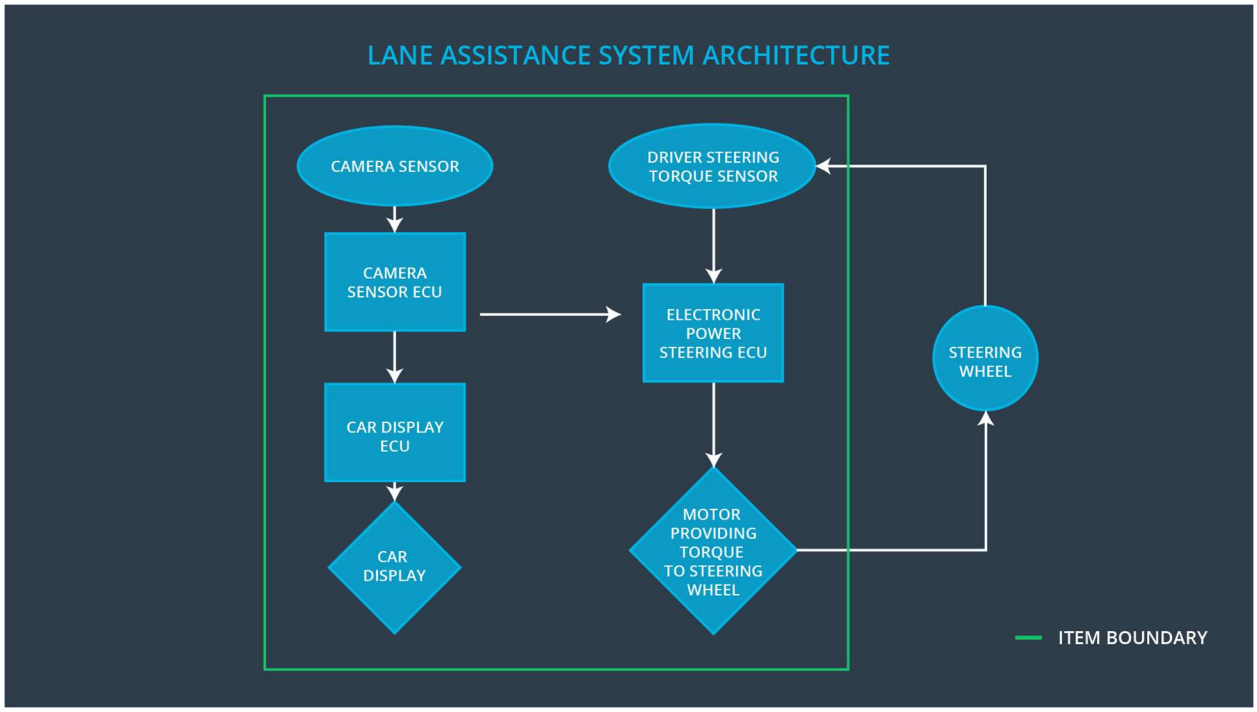
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

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 steering torque from the lane departure warning function shall be limited
Safety_Goal_02	lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver ca not 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	Detecting lane lines
Camera Sensor ECU	Determining when the vehicle leaves the lane and calculating a vibrating steering torque request for lane departure warning or assistive steering torque request for lane keeping assistant
Car Display	Displaying warning messages to driver in case of malfunctions
Car Display ECU	Controlling car display unit to display lane departure warning and lane assistance warning message
Driver Steering Torque Sensor	Measuring the torque provided by the driver
Electronic Power Steering ECU	Determining an appropriate amount of torque based on a lane assistance system torque request
Motor	Providing assistive 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 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	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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Lane departure warning function is turned off
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency	C	50ms	Lane departure warning function is turned 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	Criteria: Maximum steering torque amplitude allowed in lane departure warning Method: Test how drivers react to different torque amplitudes to prove that an appropriate value is chosen	Criteria: When the torque amplitude crosses the limit, the lane assistance output is set to 0 within the 50ms fault tolerant time interval Method: Do a software test inserting a fault into the system and see what happens
Functional Safety Requirement 01-02	Criteria: Maximum steering torque frequency allowed in lane departure warning Method: Test how drivers react to different torque frequencies to prove that an appropriate value is chosen	Criteria: When the torque frequency crosses the limit, the lane assistance output is set to 0 within the 50ms fault tolerant time interval Method: Do a software test inserting a fault into the system and see what happens

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

Lane Keeping Assistance (LKA) Requirements:

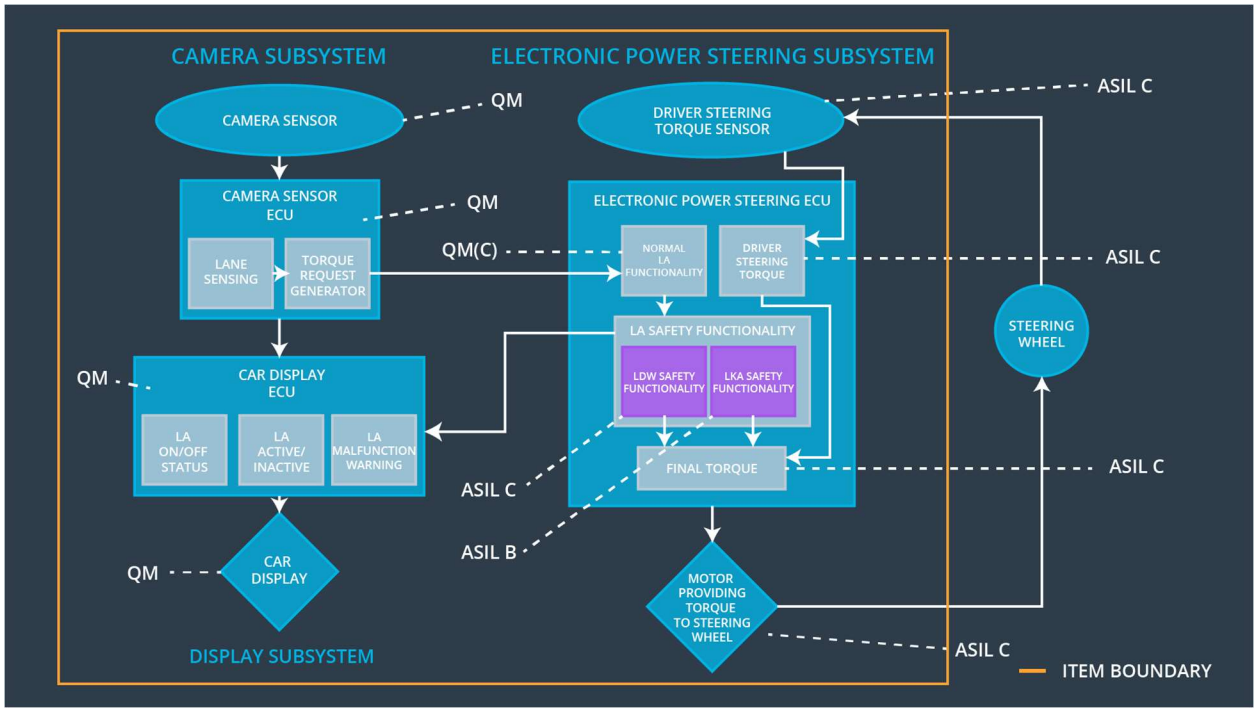
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	Lane keeping assistance is turned off

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	Criteria: Maximum duration Method: Validate that the max_duration chosen really did dissuade drivers from taking their hands off the wheel	Criteria: System really does turn off the lane keeping assistance by every exceed max_duration Verification: The system really does turn off if the lane keeping assistance ever 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 amplitude is below Max_Torque_Frequency	**X**		
Functional	The electronic power steering	**X**		

Safety Requirement 02-01	ECU shall 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	Turn off the lane departure warning functionality	The lane departure warning function applies an oscillating torque with very high torque amplitude or frequency (above limit)	Yes	Warning lights turned on to show over-applied steering torque
WDC-02	Turn off the lane keeping assistance functionality	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function	Yes	Warning light to show that the lane keeping assistance functionality is not meant for autonomous driving