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
13.12.2017	1.0	Dhanasekaran	Initial version
18.12.2017	2.0	Dhanasekaran	Update based on Udacity review comments

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

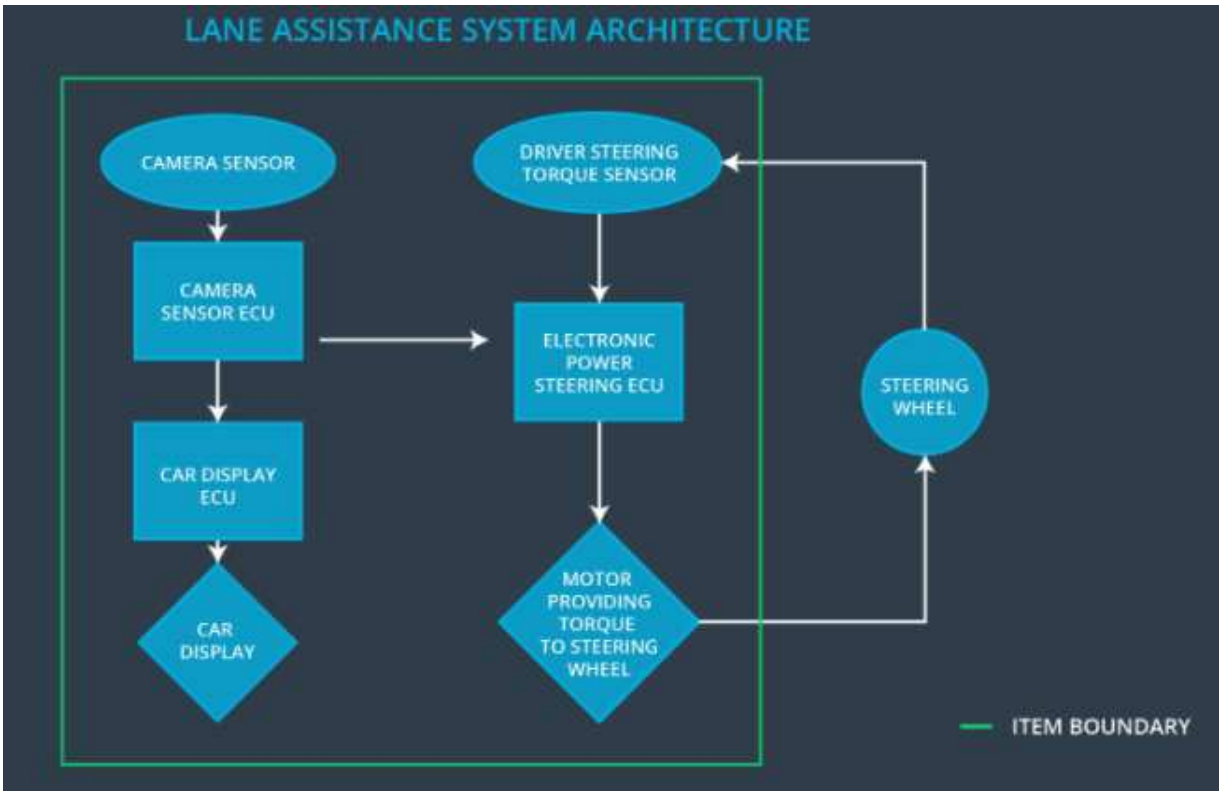
The purpose of the functional safety concept is to document the functional safety requirements that are derived from safety goals and allocating them to system architectural element

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal	ASIL
Safety_Goal_01	The oscillating torque from the lane departure warning function shall be limited	ASIL C
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.	ASIL B
Safety_Goal_03	The lane keeping assistance function shall apply correct amount of required torque to bring back the vehicle to the ego lane center	ASIL C
Safety_Goal_04	The lane keeping assistance function shall apply torque in the correct direction to bring back the vehicle to the ego lane center	ASIL C

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Takes images of the road
Camera Sensor ECU	Detecting lane lines and determining when the vehicle leaves the lane
Car Display	Displays the warning messages to driver
Car Display ECU	Determines what warning messages to be displayed and transfers it to Car Display
Driver Steering Torque Sensor	Measures the torque at the steering wheel
Electronic Power Steering ECU	Calculates the amount of torque to be applied to the steering wheels and correspondingly generated the required current for the motor

Motor	Physically generates the torque requested by the 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

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
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque	WRONG	The lane keeping assistance function adds torque in the wrong direction

	when active in order to stay in ego lane		

Functional Safety Requirements

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	Switch off LDW functionality
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below "Max_Torque_Frequency"	C	50ms	Switch off LDW functionality

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	**Acceptance Criteria :** MAX_Torque_Amplitude being high enough to be detected by the driver, but low enough not to cause loss of steering **Method:** vehicle level validation	**Acceptance Criteria :** The amplitude of the torque generated by power steering ECU shall not exceed validated Max_Torque_Amplitude **Method:** Fault injection test at vehicle level
Functional Safety Requirement 01-02	**Acceptance Criteria :** MAX_Torque_Frequency being high enough to be detected by the driver, but low enough not to cause loss of steering **Method:** vehicle level validation	**Acceptance Criteria :** The frequency of the torque generated by power steering ECU shall not exceed validated Max_Torque_Frequency **Method:** Fault injection test at vehicle level

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

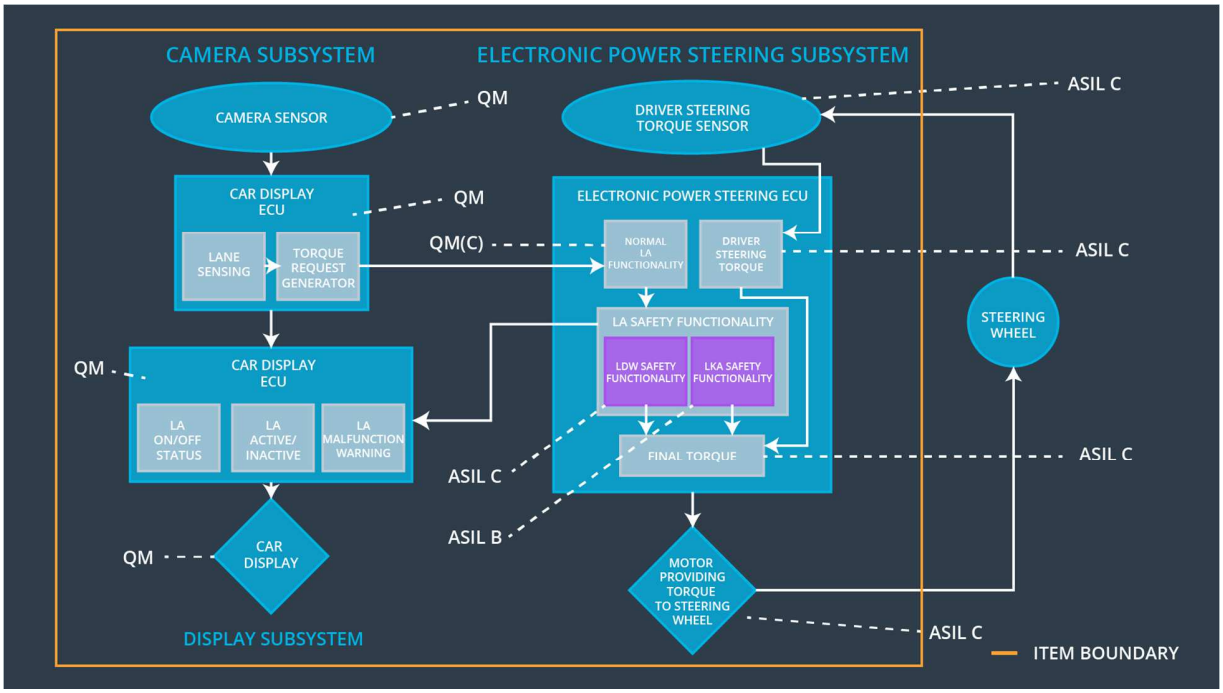
Lane Keeping Assistance (LKA) Requirements:

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	Switch off LKA functionality
Functional Safety Requirement 02-03	The electronic power steering ECU shall ensure that the additional lane keeping assistance torque is applied in the same direction as steering wheel movement	C	50ms	Switch off LKA functionality

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	**Acceptance Criteria :** Max_Duration shall be sufficient enough to provide enough feedback to driver and simultaneously not allowing him/her to misuse as Autonomous driving **Method:** Validation at vehicle level	**Acceptance Criteria :** the LDW function shall deactivate after MAX_Duration **Method:** testing at vehicle level
Functional Safety Requirement 02-03	**Acceptance Criteria :** The direction of the additional torque shall be always in the same direction as steering wheel **Method:** Validation at vehicle level	**Acceptance Criteria :**test whether the direcion of additional torque is same as that of the steering wheel direction **Method:** testing at vehicle level

Refinement of the System Architecture



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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below “Max_Torque_Amplitude”	**X**		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below “Max_Torque_Frequency”	**X**		

Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	**X**		
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the correct amount of lane keeping assistance torque is applied	**X**		
Functional Safety Requirement 02-03	The electronic power steering ECU shall ensure that the of lane keeping assistance torque is applied in the right direction	**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	Turn off the LDW functionality	When the following functional safety requirements are not met "Functional Safety Requirement 01-01" "Functional Safety Requirement 01-02"	Yes	A blinking warning signal is displayed in the instrument cluster and an acoustic warning is also provided
WDC-02	Turn off the LKA functionality	When the following functional safety requirements are not met "Functional Safety	Yes	A blinking warning signal is displayed in the instrument cluster and an acoustic warning is also provided

		Requirement 02-01” “Functional Safety Requirement 02-02” “Functional Safety Requirement 02-03”		