Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
23/5/2018	1.0	Vivek Pathak	First Attempt
25/5/2018	1.1	Vivek Pathak	Second Attempt

Table of Contents

Purpose of the Functional Safety Concept

Functional safety basically looks into the safety concepts without involving much into its technical concepts of the systems. As it basically concerned with the safety concepts that are accepted at the society

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

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 thus after lane change control should be given back to driver

Preliminary Architecture

Description of architecture elements

Element	Description
Camera Sensor	Capture images and feed them to the Camera Sensor ECU.
Camera Sensor ECU	Detect lane lines and position of the car with respect to lane
Car Display	Provide feedback to the driver displaying warnings and the Lane Departure Assistance status.
Car Display ECU	It controls the display unit of car and based on input the received from other inputs.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by

	the driver.
Electronic Power Steering ECU	It takes input from Driver Steering Torque Sensor and camera ECU and decide on amount of torque applied on steering wheel.
Motor	Applies the torque indicated by the Electronic Power Steering ECU 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

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 lead to misuse as an

			autonomous driving function.

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	LDW shall ensure lane departure oscillating torque amplitude be below the Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	LDW shall ensure lane departure oscillating torque frequency be below the Max_Torque_Frequency.	C	50 ms	Vibration frequency is below Max_Torque_Frequency.

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 chosen is high enough to warn driver while low enough not to cause loss of steering	Check whether systems are turned off when Max_Torque_Frequency is exceed.
Functional Safety Requirement 01-02	The Max_Torque_Amplitude chosen is high enough to warn the driver and not cause the loss of steering.	Check whether systems are turned off when Max_Torque_Frequency is exceed.

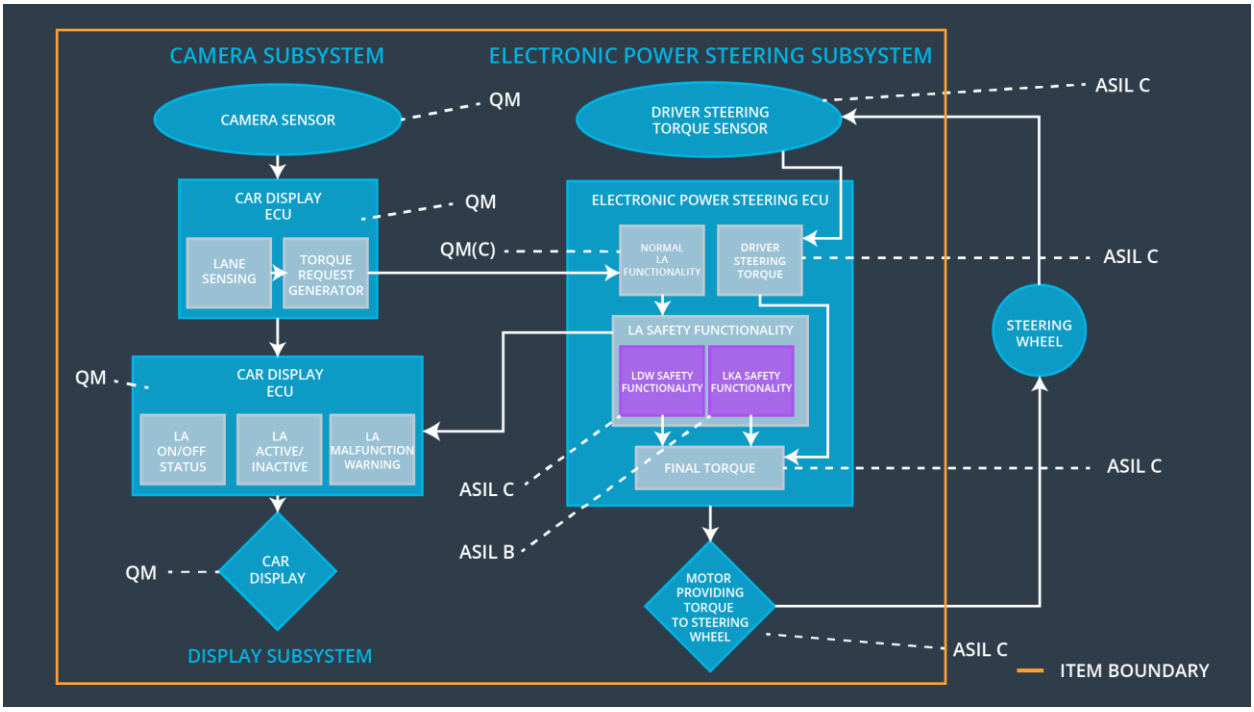
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	B	500 ms	Set LKA torque to zero

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	Validate the Max_Duration chosen not allow the driver to use the car as self-driving car.	Check whether systems are turned off if the Lane Keeping Assistance torque application exceeds Max_Duration.

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functiona l Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**Responsib le**	**Not Responsi ble**	**Not Responsible**
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**Responsib le**	**Not Responsi ble**	**Not Responsible**
Functional Safety Requirement 01-03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	**Responsib le**	**Not Responsi ble**	**Not Responsible**

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW functionality	Malfunction_01, Malfunction_02	Yes	Light displayed on dashboard and on car as warnings
WDC-02	Turn off LKA functionality	Malfunction_03, Malfunction_05	Yes	Light displayed on dashboard and on car as warnings