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
03/03/19	V1.0	Madhu Hegde	First Version

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept documents high level system requirements without going into the details. Once identified, tese requirements are allocated to different parts of the item architecture. Technical safety requirements will be derived from these safety concepts. Functional safety requirements specified with attributes in the functional safety concept. Finally requirements to validate and verify the safety requirements are specified.

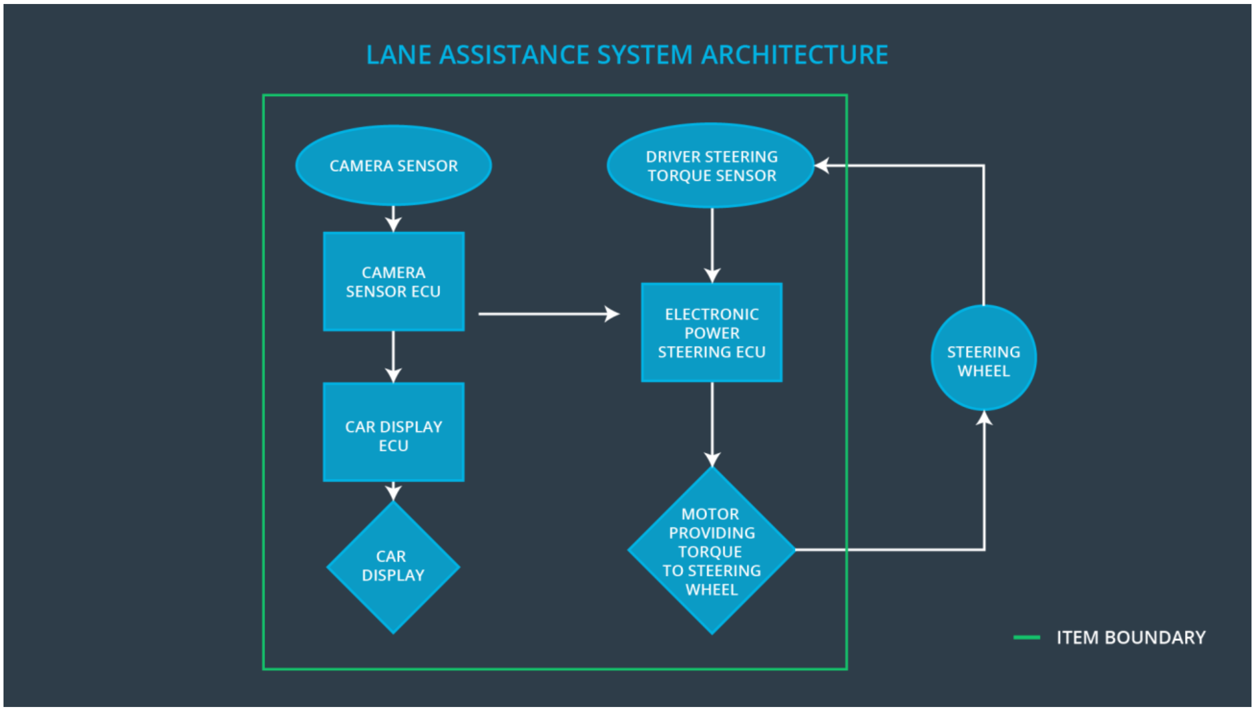
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	**Safety Goal**
Safety_Goal_01	The frequency and magnitude of vibration of steering torque from the Lane Departure Warning function shall be limited.
Safety_Goal_02	Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.
Safety_Goal_03	Lane Keeping Assistance function shall be deactivated when lanes cannot be detected due to discolored/absence of lane markings or camera malfunction
Safety_Goal_04	Lane Keeping Assistance function shall be deactivated when camera sensor cannot detect lanes due to poor visibility or camera malfunction.

Preliminary Architecture

The architecture of lane assistance system is given below


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
CAR DISPLAY
MOTOR PROVIDING TORQUE TO STEERING WHEEL
ITEM BOUNDARY

Description of architecture elements

Element	Description
Camera Sensor	Captures front facing road images and sent to Camera Sensor ECU.
Camera Sensor ECU	Performs image processing and analysis using deep neural networks or traditional Canny edge detection/Hough Transform to detect lanes and estimate car position
Car Display	Provides visual feedback regarding warnings and display Lane Departure Assistance status. The display in Tesla also shows vehicles in other lanes.
Car Display ECU	Interfaces with Camera Sensor ECU and renders processed image on the Car Display. It also shows Lane Keeping Assistance warning and Lane Departure Assistance status.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver. There are two types – sensors with contact and contact-less sensors.
Electronic Power Steering ECU	Combine the input from the Driver Steering Torque Sensor and the torque estimated by the Lane Keeping Assistance function and send final/value to the Motor. It also generates signal to the Motor to create vibrations in Steering Wheel for Lane Departure Warnings.
Motor	Received final torque calculated by the Electronic Power Steering ECU and applies 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)	NO	The Lane Keeping Assistance function is

	function shall apply the steering torque when active in order to stay in ego lane		not limited in time duration which lead to misuse as an autonomous driving function.
Malfunction _04	The Lane Departure Warning function shall be deactivated when the lanes are not detected.	WRONG	Random Lane Departure Warning display when lanes are not detected
Malfunction _05	The Lane Keeping Assistance function shall be deactivated when the lanes are not detected.	WRONG	Inconsistence steering control when Lane Keeping Assistance cannot detect lanes.

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 Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Lane Assistance Function off
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Lane Assistance Function off
Functional Safety Requirement 01-03	The Lane Departure Warning function shall be deactivated when the lanes are not detected	C	10 ms	Function is deactivated.

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	Validate Max_Torque_Amplitude chosen is high enough to be detected by a driver while low enough not to cause loss of steering	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate Max_Torque_Frequency chosen is adequate to be detected by the driver and not cause the loss of steering.	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Frequency.
Functional Safety Requirement 01-03	Validate Lane Departure Warning is off when the lanes are not detected.	Verify the Lane Departure Warning is never on when the lanes are not working.

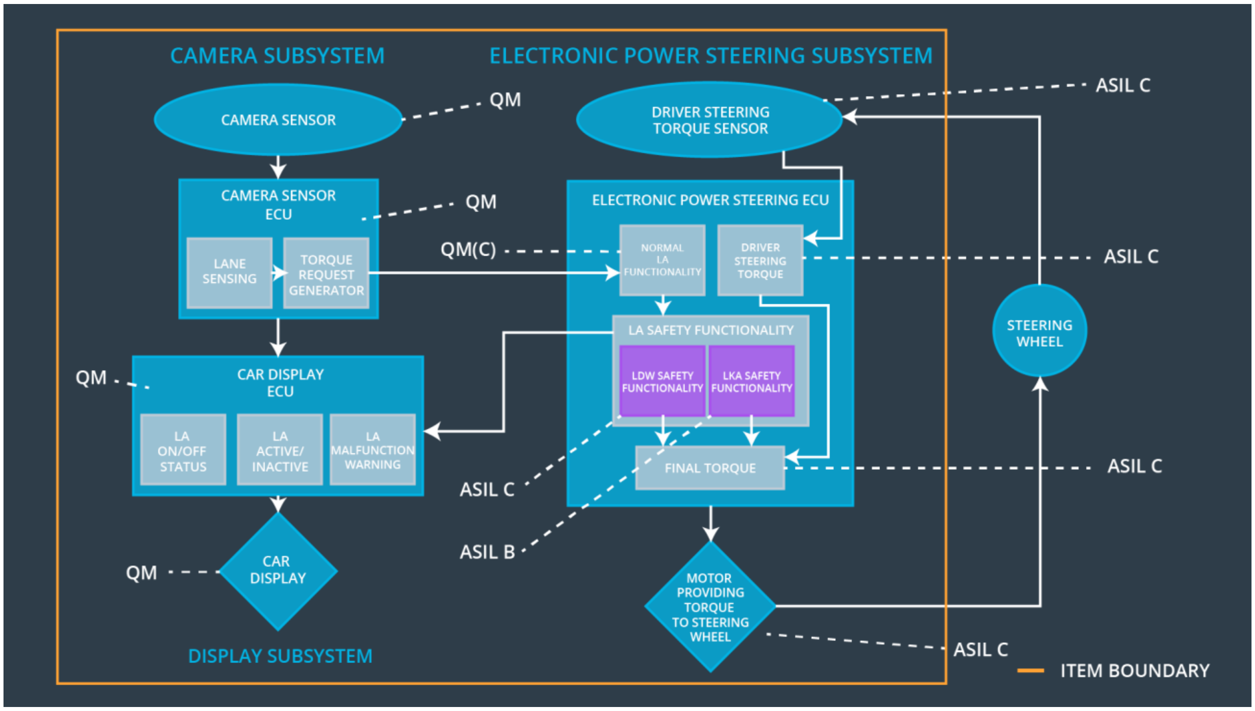
Lane Keeping Assistance (LKA) Requirements:

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 only Max_Duration.	B	500 ms	Lane Keeping Assistance torque is zero.
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working.	C	10 ms	Function is deactivated.

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 Max_Duration value to discourage the driver to use the car as autonomous driving car.	Verify the system does deactivate if the Lane Keeping Assistance torque application exceeded Max_Duration.
Functional Safety Requirement 02-02	Validate the Lane Keeping assistance shall be deactivated when the lanes are not detected	Verify the system does deactivate the Lane Keeping Assistance if the lanes are not detected.

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
Functional Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**X**		
Functional Safety Requirement 01-03	The Lane Departure Warning function shall be deactivated when the lanes are not detected	**X**		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	**X**		
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects that lanes are not detected	**X**		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on the Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_05	Yes	Lane Keeping Assistance Malfunction Warning on the Car Display