Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]
Template Version 1.0, Released on 2018-05-23

Document history

Date	Version	Editor	Description

2018-05-24	1.0	Yogesh Mahawar	First draft of Functional Safety

Table of Contents

Purpose of the Functional Safety Concept

Functional Safety document identifies high level requirements for safe system. These requirements are allocated to different parts of the item architecture. These requirements further drives requirements for Technical Safety. Instruction on how to validate and verify the requirements are presented as well.

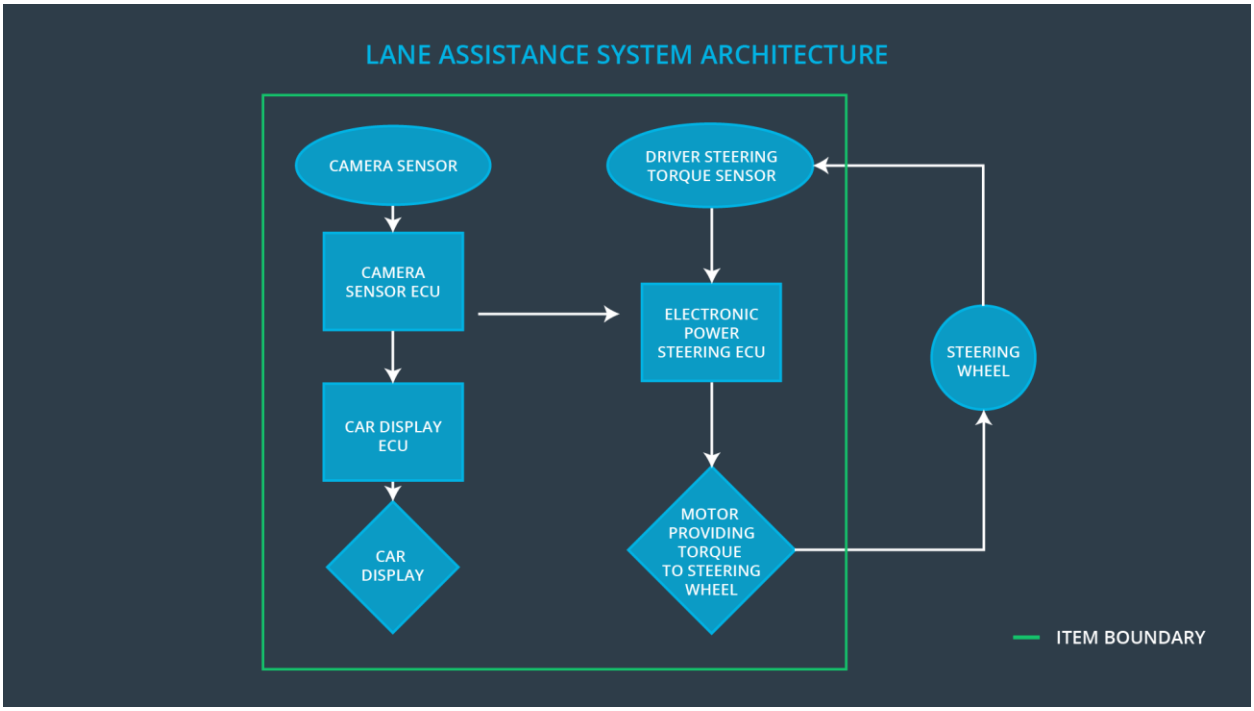
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	Oscillation steering torque from the Lane Departure Warning function shall be limited.
Safety_Goal_02	The Lane Keeping Assistance function shall be time limited, after a threshold time, torque should go off so system is not misused as Self driving.

Preliminary Architecture

Following diagram represents Architecture:



Description of architecture elements

Element	Description
Camera Sensor	Capturing and providing road images to the Camera Sensor ECU.
Camera Sensor ECU	Analyze provided images to calculate the car position on the road respect to the road lanes.
Car Display	Provide feedback to the driver, displaying warnings

	and the Lane Departure Assistance status.
Car Display ECU	Drive the Car Display component to show the Lane Keeping Assistance warning and Lane Departure Assistance status.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	Takes input from Driver Steering Torque Sensor, the torque requested by the Lane Keeping Assistance , Lane Warning and calculates the necessary torque to be applied by the Motor actuator.
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	An oscillating torque with very high torque amplitude (above limit) by Lane Departure Warning Function
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the	MORE	The Lane Departure Warning function applies an oscillating torque with very high

	driver a haptic feedback		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	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is always within limit or less then Max_Torque_Amplitude.	C	50ms	Vibration torque amplitude below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is always within limit or less then Max_Torque_Frequency.	C	50ms	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	Max_Torque_Amplitude chosen is high enough to be detected by a driver while low enough not to make drive loose control over steering wheel	The system does turn off if the Lane Departure Warning exceeded Max_Torque_Amplitude.
Functional	Max_Torque_Frequency chosen is	Verify the system does turn off if the

Safety Requirement 01-02	adequate to be detected by the driver and not cause the loss of steering.	Lane Departure Warning exceeded Max_Torque_Frequency.

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

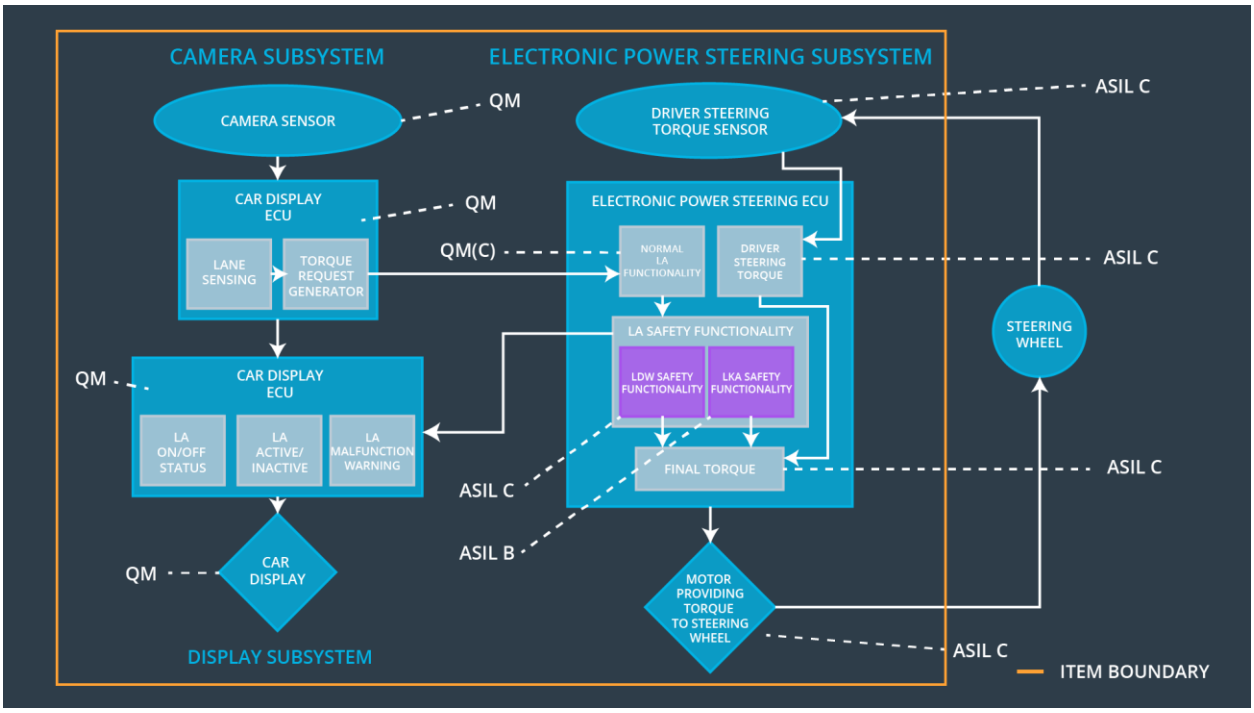
Lane Keeping Assistance (LKA) Requirements:

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 only Max_Duration.	B	500ms	After exceeding time duration Lane Keeping Assistance torque is 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.	Verify the system does deactivate if the Lane Keeping Assistance torque application exceeded 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
Functional Safety Requirement 01-01	The Lane Departure Warning item shall make sure that the lane departure oscillating torque amplitude is always below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The Lane Departure Warning item shall make sure that the lane departure oscillating torque frequency is always below Max_Torque_Frequency.	**X**		
Functional Safety	The electronic power steering ECU shall ensure that the Lane	**X**		

Requirement 02-01	Keeping Assistance torque is applied only Max_Duration.			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Steering torque frequency and/or Amplitude are degraded	Malfunction_01, Malfunction_02	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Lane keeping Assistance function will turn off	Malfunction_3	Yes	Lane keeping Assistance Malfunction Warning on Car Display