Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
05/24/18	1.0	Ganesh Prabakaran	Initial

Table of Contents

Contents

Purpose of the Functional Safety Concept

Functional Safety Concept documents the high level system requirements. These requirements are allocated to different parts of the item architecture. Technical safety requirements will be derived from these safety concepts. 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	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 additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.

Preliminary Architecture

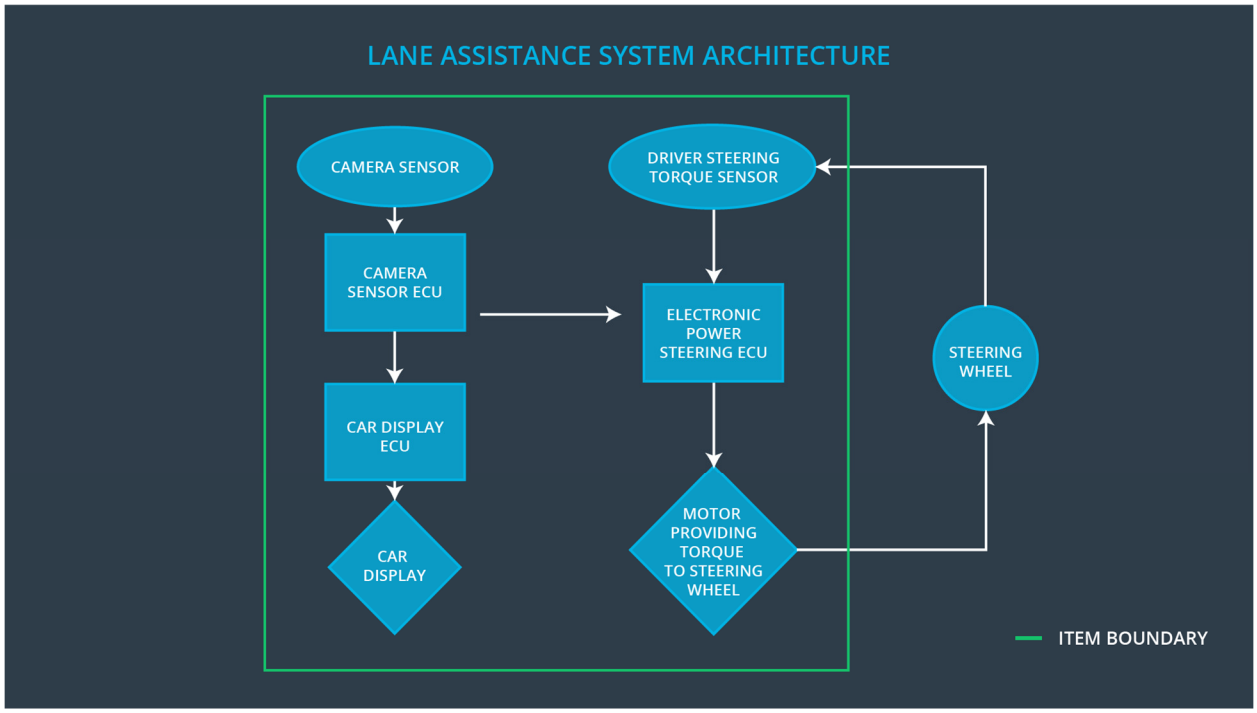

Fig 1 Lane Assistance System Preliminary Architecture
[Image source: https://udacity.com]

Description of architecture elements

Element	Description
Camera Sensor	Captures images from the front view of the car to assist in lane detection.
Camera Sensor ECU	Performs computation on the captured images to detect lanes and find the position of the car with respect to the lane
Car Display	Provides visual indication to the driver such as (1) whether the system is ON or OFF and (2) the car is steering off the lane etc
Car Display ECU	This ECU Receives input from the camera sensor ECU when the car is steering off the lane and signals the car display to turn on the warning light.
Driver Steering Torque Sensor	This sensor captures the steering wheel angular displacement initiated by the driver and sends it to the Electronic Power Steering ECU

Electronic Power Steering ECU	This ECU adds input from both driver steering torque sensor and along with the deviation compared with Camera Sensor ECU and provides steering torque amplitude to the steering wheel motor
Motor	Motor provides steering torque to the steering wheel based on the amplitude received from the Electronic Power steering 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	NO	The lane keeping assistance function is not limited in time duration which leads to misuse as

	to stay in ego lane		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 system shall ensure the lane departure oscillating torque amplitude is not exceeding Max_Torque_Amplitude.	C	50ms	Set Oscillating Torque amplitude to zero when fault is detected
Functional Safety Requirement 01-02	The lane departure warning system shall ensure the lane departure oscillating torque frequency is not exceeding Max_Torque_Frequency.	C	50ms	Set Oscillating Torque frequency to zero when fault is detected

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	Prove that the chosen value of max torque amplitude is an appropriate value. Validate by a test how drivers react to different torque amplitudes.	Verify the lane departure warning sets to zero within the 50 ms fault tolerant time interval when the torque amplitude crosses the limit. Perform a software test by inserting a fault into the system and see what happens.
Functional Safety Requirement 01-02	Prove that the chosen value of max torque amplitude is an appropriate value. Validate by a test how drivers react to different torque frequencies	Verify the lane departure warning sets zero within the 50 ms fault torlerant time when the torque frequency crosses the limit. Perform a software test by inserting a

		fault into the system and see what happens.

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	Lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving	B	50	Lane keeping assistance function should stop applying extra torque after the fault tolerant time interval

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	Test and validate that the max duration chosen really did dissuade drivers from taking their hands off the wheel.	Verify that the system really does set to zero if the lane keeping assistance every exceeded max duration.

Refinement of the System Architecture

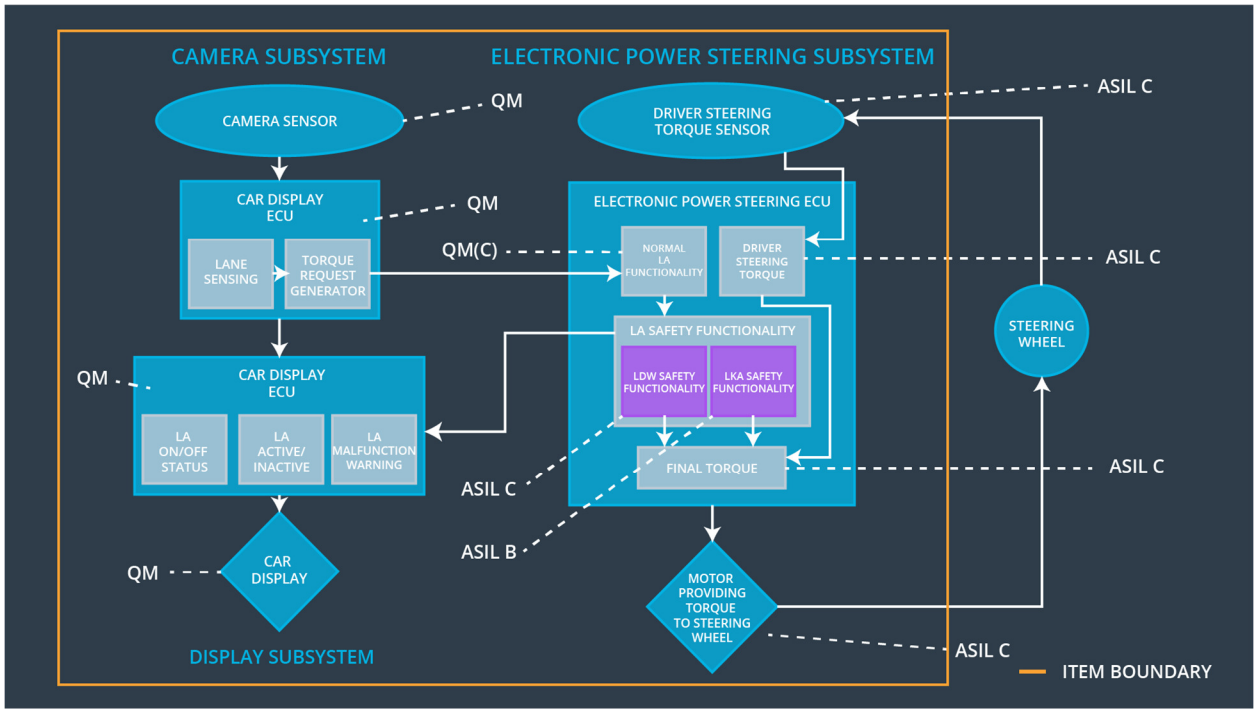

Fig 2 Refined Lane Assistance System Architecture
[Image source: https://udacity.com]

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 system shall ensure the lane departure oscillating torque amplitude is not exceeding Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The lane departure warning system shall ensure the lane departure oscillating torque amplitude is not exceeding Max_Torque_Frequency.	**X**		

Functional Safety Requirement 02-01	Lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane Departure Functionality set to zero	Malfunction_01, Malfunction_02	Yes	Lane Departure Malfunction warning on display
WDC-02	Lane Keeping Assistance Functionality set to zero	Malfunction_03	Yes	Lane Keeping Assistance Malfunction warning on display