Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
21/10/2018	1.0	L.R	First Submission

Table of Contents

Purpose of the Functional Safety Concept

This document first determines which sub-systems and elements of the Lane Assistance System can be used to meet safety goals. The safety goals determined in the Hazard Analysis and Risk Assessment are refined into Functional Safety Requirements, and allocated to the relevant sub-systems in the system architecture. The Functional Safety Concept is used to develop the Technical Safety Requirements. Verification and Validation for functional requirements is discussed 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 torque from the lane departure warning shall be limited
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
Safety_Goal_03	Deactivate LKA if in reverse
Safety_Goal_04	System deactivates if driver torque is opposite direction to LKA torque

Preliminary Architecture

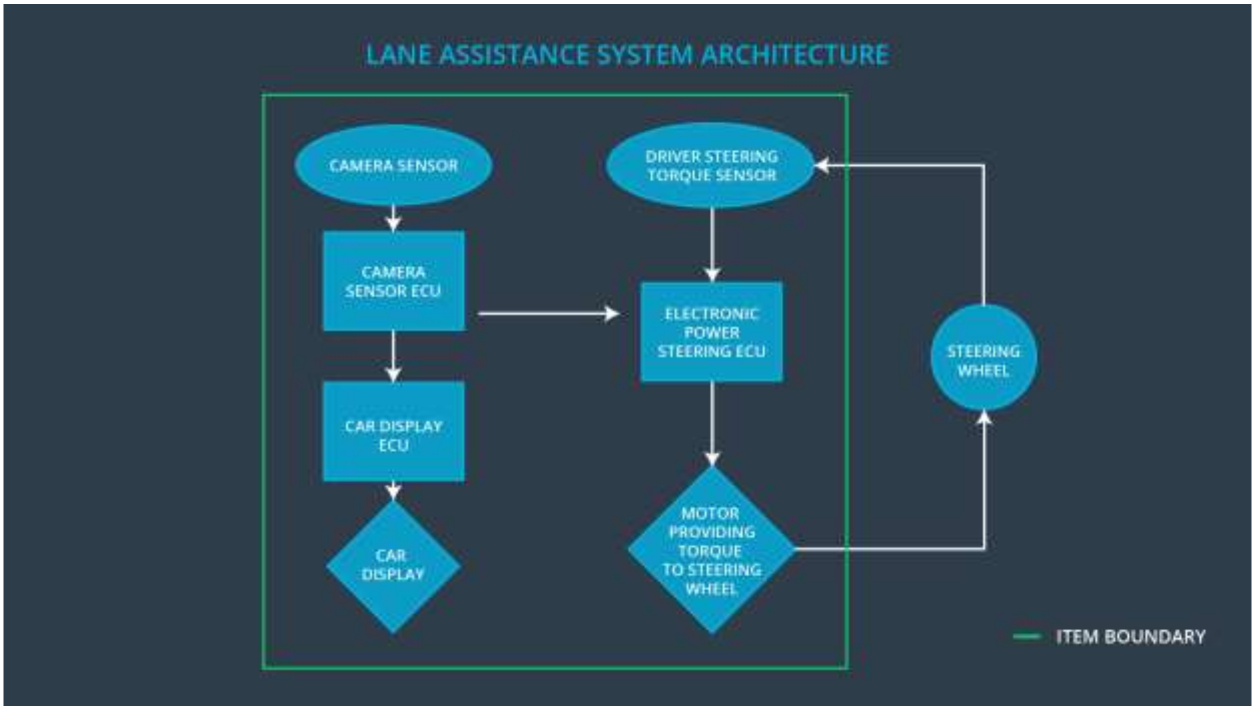
LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

Figure 1 - Preliminary system architecture for Lane Assistance System

Description of architecture elements

Element	Description
Camera Sensor	Takes images of the road and passes them to the Camera Sensor ECU.
Camera Sensor ECU	Detects lane lines and determines car position relative to center of lane. Sends warnings to Car Display and torque commands to EPS ECU.
Car Display	Displays feedback to the driver about lane departure warnings and other system status.
Car Display ECU	Drives the display based on information received from camera ECU
Driver Steering Torque Sensor	Measure torque applied to steering wheel by driver and sends measurement to EPS ECU
Electronic Power Steering ECU	Input: Driver torque, Camera requested torque Output: extra torque required to steer the car back onto the center of the lane.
Motor	Applies torque to steering wheel as commanded by

	EPS 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 LDW function applies too high oscillating torque amplitude to the steering wheel (above limit).
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The LDW function applies too high oscillating torque frequency to the steering wheel (above limit).
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	LKA was always on and had no time limit, so drivers could take both hands off the wheel.

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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Turn system off
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Turn system off

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	Test how drivers react to different torque amplitudes to prove that we chose an appropriate value.	Software test inserting a fault into the system and seeing what happens.
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that we chose an appropriate value.	Software test inserting a fault into the system and seeing what happens.

[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 lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	Turn system off

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 with drivers that the max_duration chosen really did dissuade drivers from taking their hands off the wheel	Test that the system really does turn off if the lane keeping assistance every exceeded max_duration

Refinement of the System Architecture

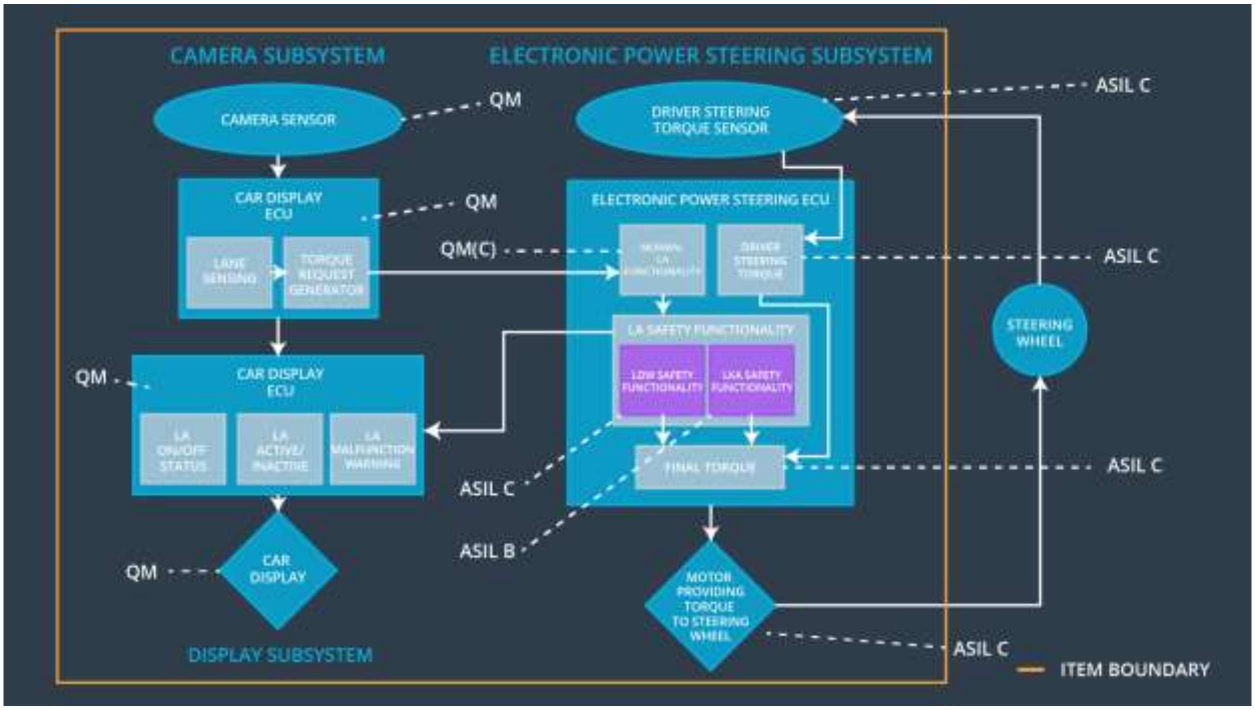

Figure 2 - Refined system architecture diagram for Lane Assistance System

Allocation of Functional Safety Requirements to Architecture Elements

ID	**Functional Safety Requirement**	**Electronic**	**Camera**	**Car Display**

		Power Steering ECU	ECU	ECU
Functional Safety Requirement 01-01	The EPS ECU shall ensure that the LDW oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The EPS ECU shall ensure that the LDW oscillating torque frequency is below Max_Torque_Frequency	**X**		
Functional Safety Requirement 02-01	The EPS ECU shall ensure that the LKA torque is applied only for Max_Duration	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	turn off the functionality	Malfunction_01 Malfunction_02	Yes	Car display will show fault
WDC-02	turn off the functionality	Malfunction_03	Yes	Car display will show fault