Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: Version 3.0

Document history

Date	Version	Editor	Description

29/10/2017	1.0	Adriana Costas	First attempt
20/11/2017	2.0	Adriana Costas	Second attempt
06/12/2017	3.0	Adriana Costas	Third attempt

Table of Contents

Purpose of the Functional Safety Concept

The purpose of the functional safety concept is to provide a high-level conceptual description of how the safety goals identified in the HARA document will be achieved and to allocate them to the preliminary architectural elements of the item (or to external measures).

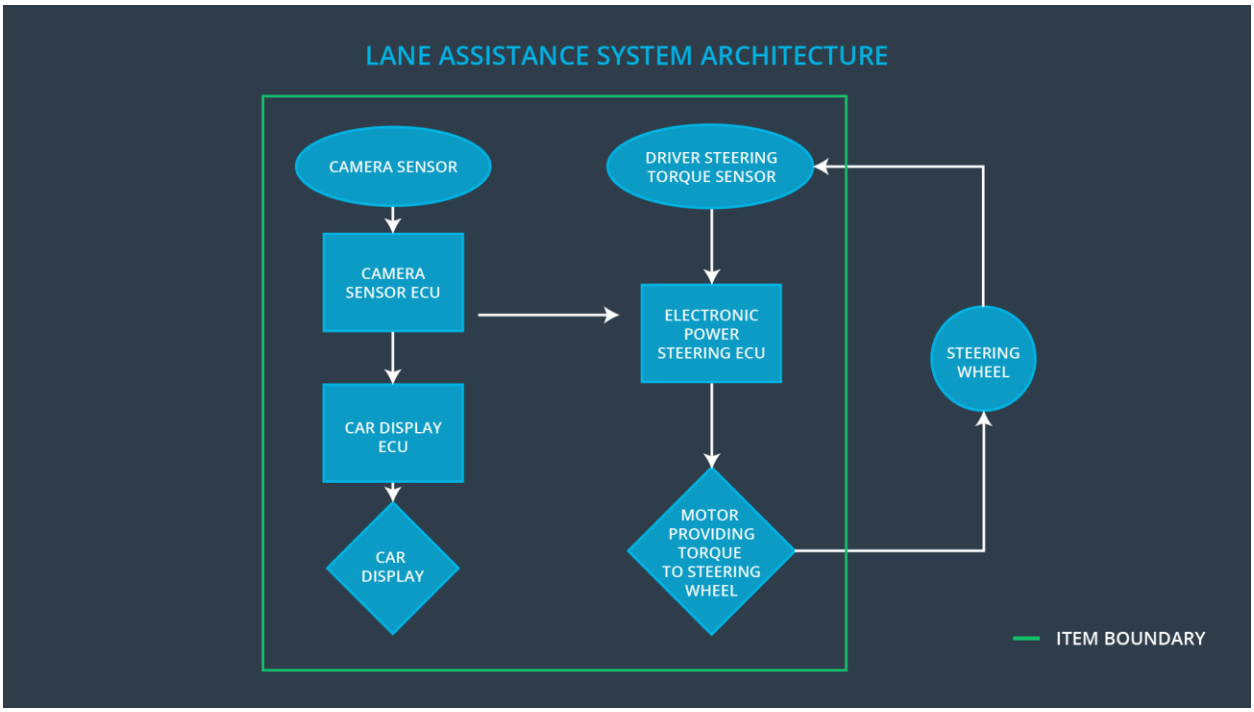
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating torque to the steering wheel from the lane keeping assistance function shall be limited
Safety_Goal_02	The lane keeping assistance (LKA) 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	The camera sensor ECU shall check the LA on/off, active/inactive and malfunction warning status before sending torque requests to the lane departure warning system

Safety_Goal_04	The lane keeping assistance (LKA) function shall deactivate when the camera sensor stops detecting road markings and shall warn the driver of its deactivation.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Sensor responsible for capturing vehicle driving condition including detectable lane lines.
Camera Sensor ECU	Electronic Control Unit (ECU) responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
Car Display	Visual display responsible to displaying warning of lane departures and LKA activation and deactivations.
Car Display ECU	Electronic control unit (ECU) resposible for displaying warning of lane departures and LKA and LDW activation and deactivation on the Car display.
Driver Steering Torque Sensor	Sensor resposible for measuring how much force

	(steering torque) the driver is applying to the steering wheel.
Electronic Power Steering ECU	Electronic Control Unit (ECU) responsible for measuring the torque provided by the driver and adding appropiate amount of torque based on a lane assitance system torque request (LKA) and vibrates the steering wheel when the driver drifts away from center by mistake (LDW)
Motor	Actuator responsible for applying requested torque to the steering column by the Electronic Power Steering ECU for either the LKA or the LDW functions.

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

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 leads to misuse as an autonomous driving function.
Malfunction_04	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver with haptic feedback.	WRONG	The lane departure warning function unexpectedly activates and starts oscillating the steering wheel during normal city driving.
Malfunction_05	Lane Keeping assistance (LKA) function shall apply the steering torque when activate in order to stay in ego lane	WRONG	The lane keeping assistance function is not able to detect lane markings in darken tunnel

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	50 ms	Set vibration torque amplitude to zero
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	Set vibration torque frequency to zero.

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 driver while low enough not to cause loss of steering	Verify that the system really does turn off if the lane departure warning ever exceeded MAX_Torque_Amplitude
Functional Safety Requirement 01-02	Validate MAX_Torque_Frequency chosen is high enough to be detected by driver while low enough not to cause loss of steering.	Verify that the system really does turn off if the lane departure warning ever exceeded MAX_Torque_Frequency.

Lane Keeping Assistance (LKA) Requirements:

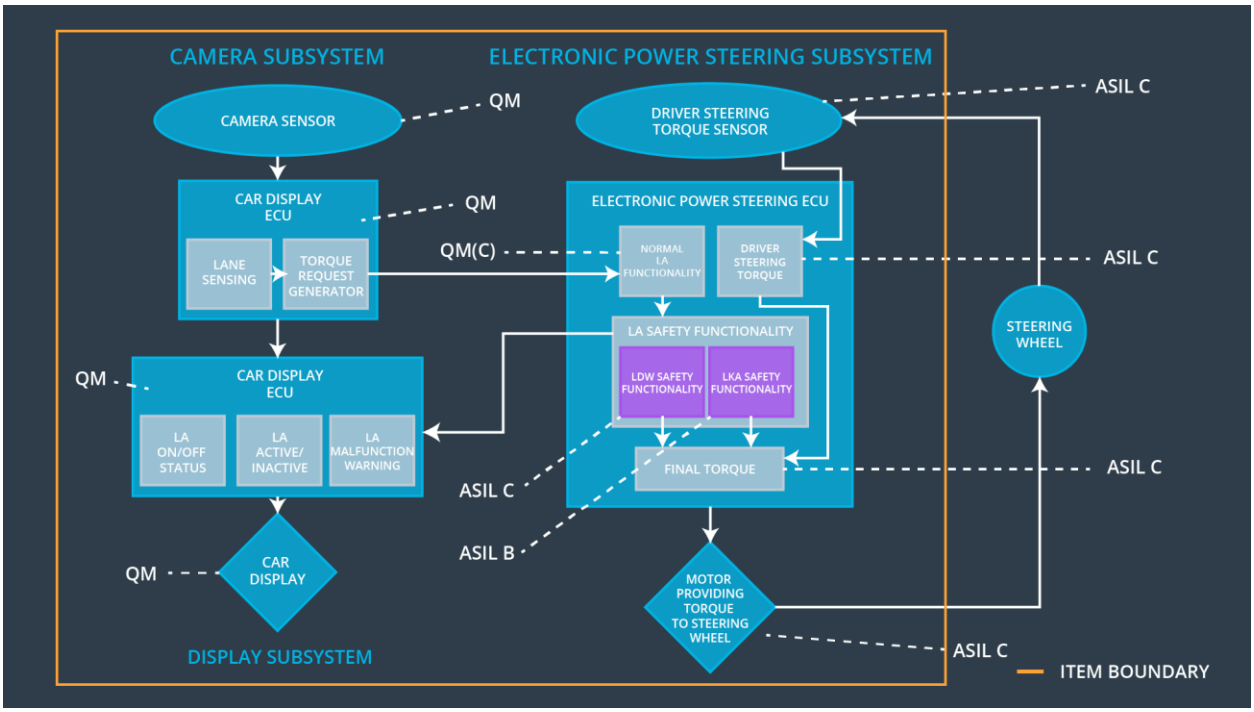
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	Set lane keeping assistance torque to zero
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU stops detecting road markings and shall send its off status to Car Display	B	500 ms	Set lane keeping assistance 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 that the MAX_Duration chosen really dis dissuade drivers from taking their hands off the wheel	Verify that the system really does turn off if the lane keeping assistance ever exceeded Max_Duration
Functional	Validate Camera sensor ECU does not	Verify that the system really does turn

Safety Requeriment 02-02	generate torque request when lane sensing is lost.	off if the camera sensor ECU ever loses road marking detection.

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 Keeping item shall ensure that the lane departure oscillating torque amplitude is below MAX_Torque_Amplitude	**x**		
Functional Safety Requirement	The Lane Keeping item shall ensure that the lane departure oscillating torque frequency is	**x**		

01-02	below MAX_Torque_Frequency			
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	**x**		
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU stops detecting road markings and shall send its off status to Car Display	**x**		

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	Lane Assist Inactive and Malfunction Warning will be set in the Car Display ECU
WDC-02	Turn off LKA functionality	Malfunction_03, Malfunction_04	Yes	Lane Assist Inactive and Malfunction Warning will be set in the Car Display ECU