Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 2.0
Released on 2017-09-08

Document history

Date	Version	Editor	Description
Sep 01, 2017	1.0	Sampath Vanimisetti	Initial draft.
Sep 08, 2017	2.0	Sampath Vanimisetti	

Table of Contents

Contents

Purpose of the Functional Safety Concept

Functional safety concept looks at the item at a higher level of abstraction. The purpose of function safety concept is to define high-level requirements, and does not cover the technical aspects of safety (hardware, sensors, algorithms, etc). At a high-level, the functional safety concept assigns these requirements to the system diagrams. For example, to achieve ISO 26262 standard, aspects related to potential malfunctions of lane assistance systems are defined in this document at high-level.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	For lane departure warning (LDW), audible, visual and tactile feedback is given to driver. For tactile feedback, steering motor is used to generate vibration at steering wheel. The oscillating torque at steering wheel should be limited by software to ensure safe operation.
Safety_Goal_02	In order to prevent lane keep assistance (LKA) item being misused as autonomous system, the electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only short duration (for example, no more than 5 seconds).
Safety_Goal_03	Lane keep assistance (LKA) shall deactivate in the event that the camera cannot see the road ahead. This may be due to inadvertent blockage of line-of-sight or poor environmental conditions (rain, snow, fog, etc).
Safety_Goal_04	Power-on self-diagnostics for LDW and LKA should ensure that communication with other control modules is proper. Driver shall be warned if fault is detected and item use shall be prevented.

Preliminary Architecture

An overview of the preliminary architecture of the system is shown below in Figure 1.

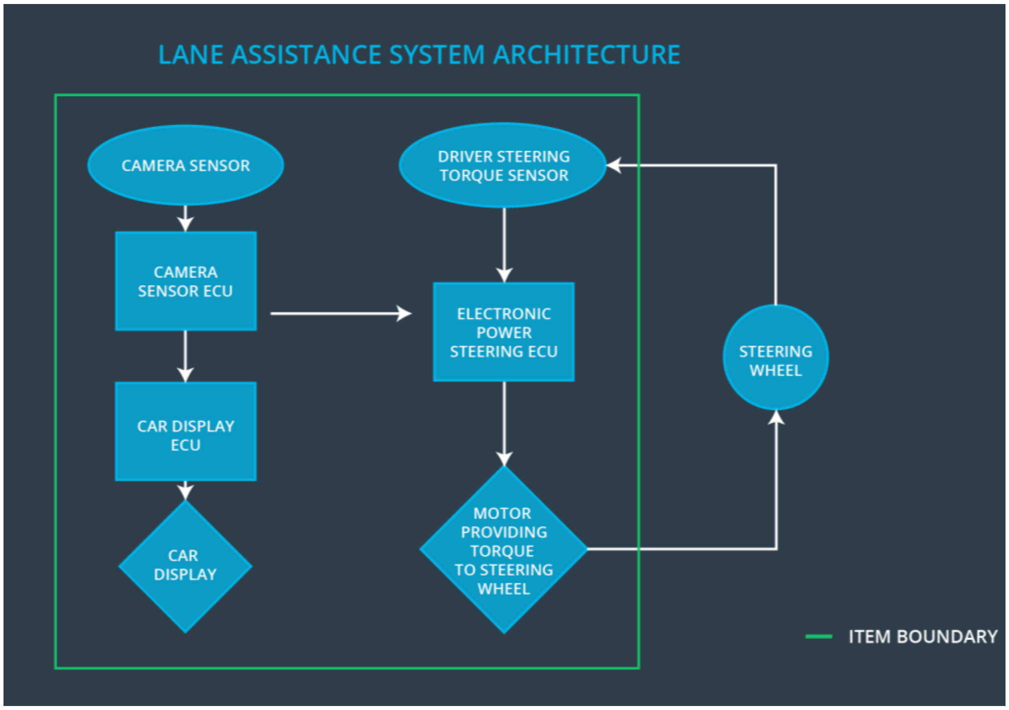
LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
CAR DISPLAY
MOTOR PROVIDING TORQUE TO STEERING WHEEL
ITEM BOUNDARY

Figure1: Preliminary architecture of the lane assistance system

Description of architecture elements

Element	**Description**
Camera Sensor	Sense or capture the view of the road in front of the vehicle. The camera sensor outputs the raw video frame feed to the camera sensor ECU.
Camera Sensor ECU	Process the raw video frame feed provided by the camera sensor and identify regions-of-interest (ROIs) from each image frame. This will include identification of the lane marking on the road. The ECU will determine the current position of vehicle in the ego-lane, distance to each lane marking and the curvature of the road ahead of the vehicle.
Car Display	Provide status and feedback for lane assistance items to the driver.
Car Display ECU	Interface with camera and sensor ECU to process incoming information and give audible/visual alters to driver.
Driver Steering Torque Sensor	Sense the torque being applied by the driver on the steering wheel. Also, encode and transmit the current steering angle back to steering control ECU.

Electronic Power Steering ECU	EPS ECU receives data from steering torque sensor, steering angle sensor and the camera sensor ECU to determine how much steering torque to apply to steering wheel. Depending on whether LDW or LKA feature is selection, it sends the relevant control signal to steering motor.
Motor	Receive commands from electronic power steering ECU and apply required torque amplitude and frequency for prescribed duration.

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: DV04 - Actor effect (amplitude) is too much	LDW applies steering oscillating torque above the maximum value
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE: DV04 - Actor effect (frequency) is too much	LDW function applies steering oscillating frequency above maximum value.
Malfunction_03	Lane Departure Warning (LDW) function shall apply	WRONG: DV02 - Function unexpectedly	Activated unexpectedly during

	an oscillating steering torque to provide the driver with haptic feedback	activated	normal driving condition.
Malfunction_04	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver with haptic feedback	LATE: DV07 – Actor action is too late	LDW alert issued too late
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO: DV03 - Function always activated limit)	LKA misused as autonomous function.
Malfunction_06	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG: DV19 - Sensor detection is wrong	LKA could not detect road lanes to center the vehicle in ego lane due to environmental conditions (rain, fog, snow, tunnel, etc).

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 01-01	LDW shall ensure that steering oscillating torque amplitude is below MAX_StrOscTrqAmp	C	50 ms	Set steering oscillation torque amplitude to zero
Functional Safety Requirement 01-02	LDW shall ensure that steering oscillating torque amplitude is below MAX_StrOscTrqFrq	C	50 ms	Set steering oscillating 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	MAX_StrOscTrqAmp is within the defined range (above minimum human detection cut-off and below maximum)	Feature / item should not shut-off when steering oscillation torque is less then MAX_StrOscTrqAmp.
Functional Safety Requirement 01-02	MAX_StrOscTrqFrq is within the defined range (above minimum human detection cut-off and below maximum)	Feature / item should not shut-off when steering oscillation frequency is less then MAX_StrOscTrqFrq.

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	LKA steering torque applied for less then duration MAX_LKAStrTrqDuration	B	500 ms	Set LKA torque value to 0
Functional Safety Requirement 02-02	LKA steering torque is set to zero upon malfunction of camera or when camera stops detecting lane markings on road	B	500 ms	Set LKA torque value to 0

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 steering torque assist was not provided to prevent driver from using it as autonomous feature.	Verify that LKA system assist turned off after MAX_LKAStrTrqDuration even if driver tried.
Functional Safety Requirement 02-02	Validate that steering torque is not generate when camera is malfunctioning or road lane markings are not visible.	Verify that steering torque values are zero when lane markings are not visible (e.g., on roads without lane markings, obstructing camera, etc)

Refinement of the System Architecture

The following Figure 2 shows the refined system architecture.

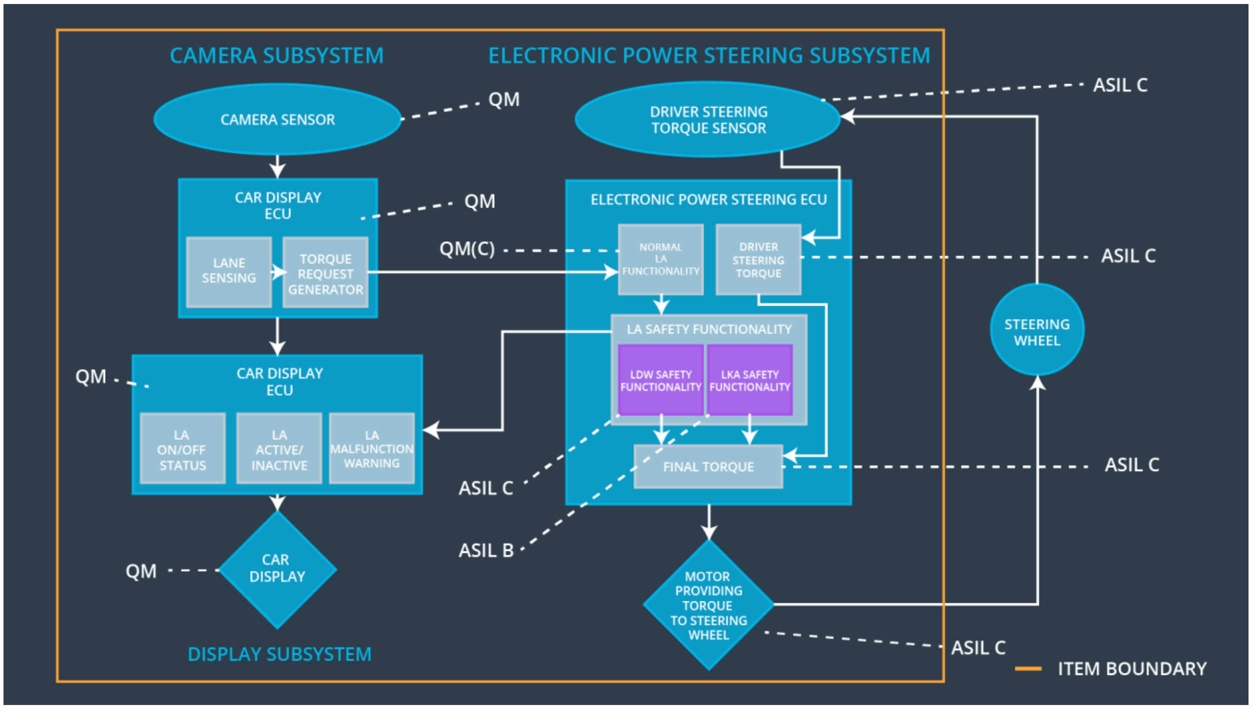

Figure 2: Overview of refined system architecture of lane assistance item.

Description of architecture elements for the refined system architecture.

Element	**Description**
Camera Sensor	Sense or capture the view of the road in front of the vehicle. The camera sensor outputs the raw video frame feed to the camera sensor ECU.
Camera Sensor ECU – Lane Sensing	Process the raw video frame feed provided by the camera sensor and identify regions-of-interest (ROIs) from each image frame. This will include identification of the lane marking on the road.
Camera Sensor ECU – Torque Request Generator	The ECU will determine the current position of vehicle in the ego-lane, distance to each lane marking and the curvature of the road ahead of the vehicle.
Car Display	Provide status and feedback for lane assistance items to the driver. For example, activation and deactivation of LDW/LKA, LDW alerts, etc.

Car Display ECU – LKA on/off status	Send signal to car display indicating LKA/LDW ON/OFF status.
Car Display ECU – LKA active/inactive status	Send signal to car display indicating LKA/LDW active/inactive status.
Car Display ECU – malfunction warning indication	Send signal to car display indicating LKA/LDW malfunction.
Driver Steering Torque Sensor	Sense the torque being applied by the driver on the steering wheel. Also, encode and transmit the current steering angle back to steering control ECU.
Electronic Power Steering ECU	Software module in EPS ECU that receives data from steering torque sensor (driver input) and steering angle sensor.
Electronic Power Steering ECU – Normal LA functionality	Software module in EPS ECU that receives data from the camera sensor ECU to determine how much steering torque to apply to steering wheel.
Electronic Power Steering ECU – LDW safety functionality	Software module in EPS ECU responsible for keeping the LDW oscillating torque amplitude and frequency below maximum prescribed values.
Electronic Power Steering ECU – LKA safety functionality	Software Module in EPS ECU responsible for limiting the LKA steering torque application duration to no more than the maximum prescribed value.
Electronic Power Steering ECU – final torque output	Software module EPS ECU responsible to receive request from LDW and LKA software modules and limit the final torque output request to below the maximum prescribed value.
Motor	Receive commands from electronic power steering ECU and apply required torque amplitude and frequency for prescribed duration.

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	Lane Assist item shall ensure that the LDW oscillating steering torque amplitude is below the MAX_StrOscTrqAmp.	**x**		
Functional Safety Requirement 01-02	Lane Assist item shall ensure that the LDW oscillating steering torque frequency is below the MAX_StrOscTrqFrq..	**x**		
Functional Safety Requirement 02-01	EPS ECU will ensure that the LKA steering torque is applied for no more than MAX_LKAStrTrqDuration	**x**		
Functional Safety Requirement 02-01	EPS ECU will ensure that LKA steering torque is set ot zero if camera malfunctions or lane marking are not visible	**x**		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn off LDW	Malfunction_01 to Malfunction_04	LDW steering osc torque amp & frq set to 0	Set LDW malfunction on car display ECU
WDC-02	Turn off LKA	Malfunction_05, Malfunction_06	LKA steering torque set to 0	Set LKA malfunction on car display ECU