Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version:
Version 1.0, Released on 2017-11-06

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
06-11-2017	1.0	S. Chonavel	Initial version

Table of Contents

Purpose of the Functional Safety Concept

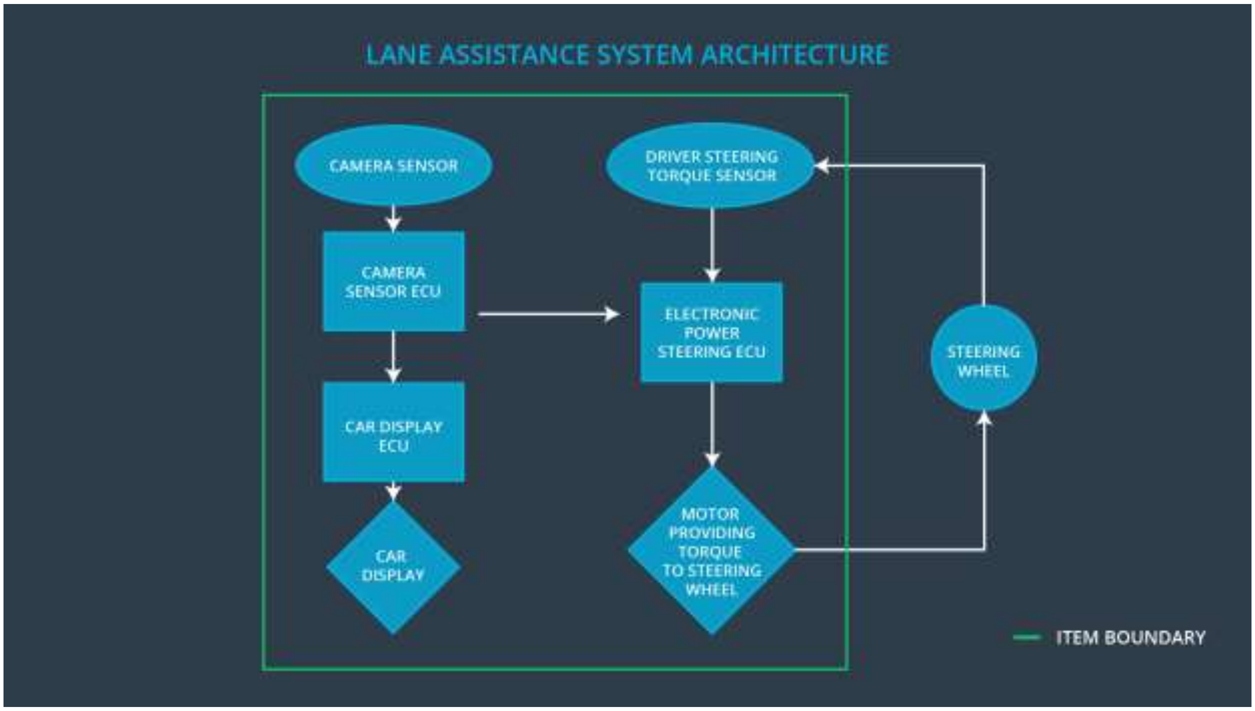
The purpose of this document is to record the system level safety goals for the “Lane Driving Assistance” item, and to allocate them to the next level down “sub system” of the system architecture, as per ISO26262 requirement.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The lane departure warning function shall apply an oscillating steering wheel torque which is within specified limits.
Safety_Goal_02	The lane keeping assistance function shall be time limited .
Safety_Goal_03	The lane keeping assistance action time shall be below a specified threshold.

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

Description of architecture elements

[

Element	Description
Camera Sensor	Capture and transmit an image of the vehicle frontal area

Camera Sensor ECU	• Analyses the camera sensor output and determine the position of the vehicle with respect to the lane. • Inform the Display System in case of lane departure. • Inform the Power Steering ECU of the lane departure situation.
Car Display	Display a lane departure signal to the driver if requested by the Camera Sensor ECU
Car Display ECU	Activate the display if activated by the Camera Sensor ECU
Driver Steering Torque Sensor	Provides steering wheel torque upon driver or camera Sensor request.
Electronic Power Steering ECU	• Provides steering torque upon driver request • Provides vibratory Line Departing Warning vibration torque upon Cameras Sensor Request • Provide Steering torque for Lane keeping Assistance upon Camera Sensor ECU request
Motor	Provides steering wheel torque upon Electronic Power Steering request.

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

[Instructions: Fill in the functional safety analysis table below.]

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 is too much	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit)
Malfunction_02	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO DV03 - Function always activated	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving Function.
Malfunction_03	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	LESS DV05 - Actor effect is too less	The lane departure warning function applies an oscillating torque with insufficient torque amplitude (bellow limit)
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	LATE DV07 - Actor action too late	The lane keeping assistance function is ineffective.

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 oscillating steering wheel torque shall be below a specified limits.	C	50ms	Set vibration torque amplitude to zero. Warn user of LDW malfunction

Functional Safety Requirement 01-02	The oscillating steering wheel torque shall be above a specified limits.	B	50ms	Set vibration torque amplitude to zero Warn user of LDW malfunction

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	Check the Steering _Wheel_Torque is less than Max_Steering_Wheel_torque	If Steering _Wheel_Torque is greater than Max_Steering_Wheel_torque then the system is turned off.
Functional Safety Requirement 01-02	Check the Steering _Wheel_Torque is lmore than Min_Steering_Wheel_torque	If Steering _Wheel_Torque is lower than Min_Steering_Wheel_torque then the system is turned off.

Lane Keeping Assistance (LKA) Requirements:

ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 02-01	The lane keeping Assistance shall be limited in time.	B	50ms	System is turned off. Warn user that LKA function is off
Functional Safety Requirement 02-02	The lane keeping assistance shall apply torque within a limited time frame.	B	50ms	System is turned off. Warn user of LKA malfunction

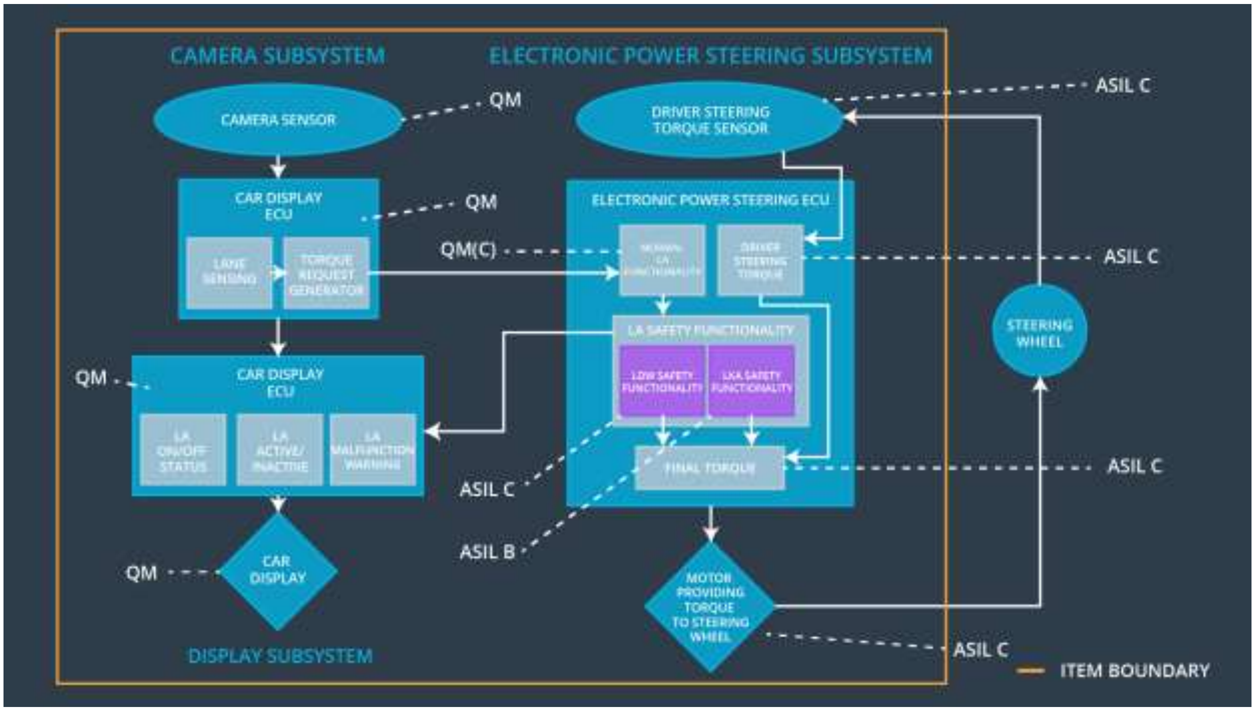
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	**Validation Acceptance Criteria and Method**	**Verification Acceptance Criteria and Method**

Functional Safety Requirement 02-01	Check LKA_active_time is lower than Max_LKA_active_time.	If LKA_active_time is greater than Max_LKA_duration, - the system is turned off (LKA_status = False) - The user is warned of the LKA state (LKA_Display_warning = True)
Functional Safety Requirement 02-02	Check LKA_action_time is lower than Max_LKA_action_time.	if LKA_action_time is greater than Max_LKA_action_time, - the system is turned off (LKA_status = False) - The user is warned of the LKA state (LKA_Display_warning = True)

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 oscillating steering wheel torque shall be below a specified limits.	**YES**		
Functional Safety Requirement 01-02	The oscillating steering wheel torque shall be above a specified limits.	**YES**		
Functional Safety Requirement 02-01	The lane keeping Assistance shall be limited in time.	**YES**		
Functional Safety Requirement 02-02	The lane keeping assistance shall apply torque within a limited time.	**YES**		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	LDW function is off	Malfunction 01-01,01-02	Yes LDW is off	Yes
WDC-02	LKA function is off	Malfunction 02-01,02-02	Yes LKA is off	Yes