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
21/5/2018	0.1	Ujjwal Saxena	Initial draft
24/5/2018	1.0	Ujjwal Saxena	Finalized document

Table of Contents

Purpose of the Functional Safety Concept

Purpose of functional safety concept is to describe the implementation of the independent safety solutions for a defined item from a higher level without delving into the technical details of the system. The primary focus here is to reduce the risks below than acceptable levels.

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 system shall be time limited, thus after a lane keeping maneuvers, the control is given back to the driver so that it can’t be misused.
Safety_Goal_03	The Lane detection system shall not be activated if the detection for a certain environment is not available.

Preliminary Architecture

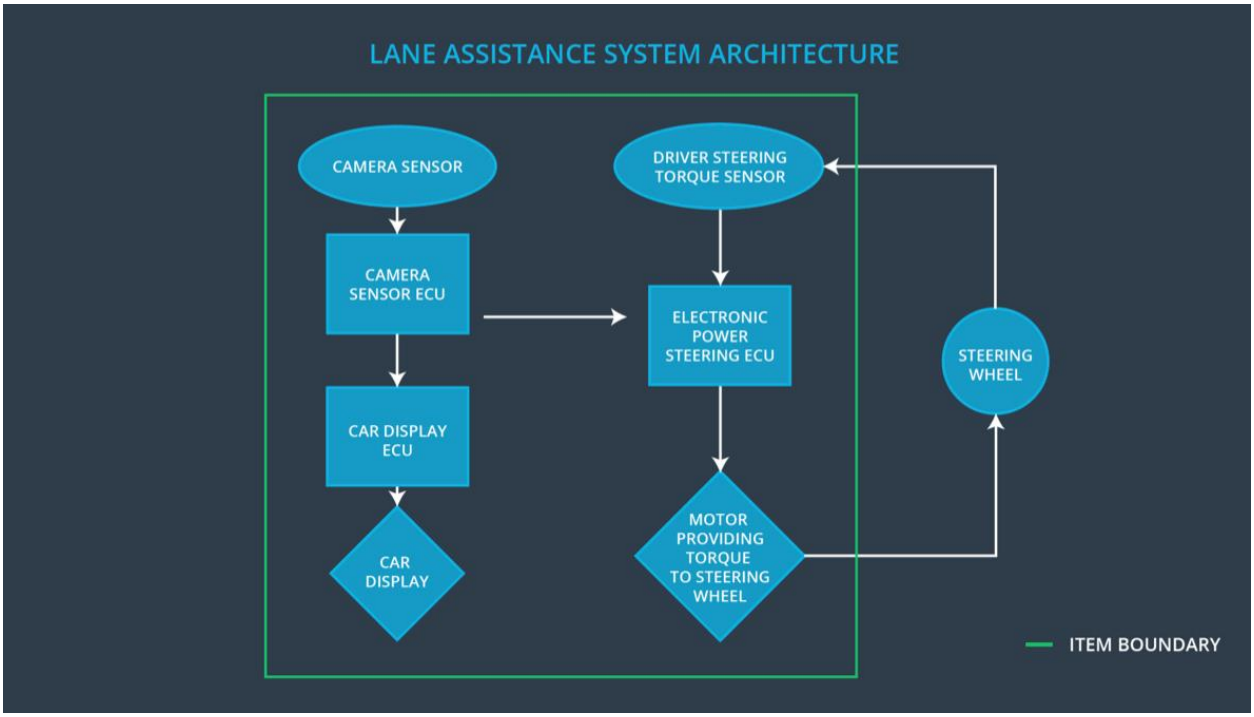

Figure 1Lane Assistance System Architecture

Description of architecture elements

Element	Description
Camera Sensor	Sensors to capture environmental information as images and provide them to the camera sensor ECU continuously.
Camera Sensor ECU	A processor unit to process acquired images by camera sensors to detect Lane Lines and calculate car positions w.r.t. to lane lines.
Car Display	Display device to display system status and warnings during system malfunctions to driver.
Car Display ECU	A processor chip controlling car displays by processing data from the camera sensor ECU.
Driver Steering Torque Sensor	Sensor to measures the torque applied to the steering wheel.

Electronic Power Steering ECU	A processor chip for processing data from camera sensor ECU and torque sensor.
Motor	An electric motor that interpret the EPS ECU data to control the steering wheel

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	LDW function applies oscillating torque of a very high (above limit) **amplitude**.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	LDW function applies oscillating torque of a very high (above limit) **frequency**.
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	The LKA doesn't have a time limiting function resulting in its misuse as 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 keeping item shall ensure that the lane departure warning torque **amplitude** is below **Max_Torque_Amplitude**	C	50ms	set torque to zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure warning torque **frequency** is below **Max_Torque_Frequency**	C	50ms	set torque 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	Set the value of Max_Torque_Amplitude such that it is adequate enough to warn the driver without causing steering loss.	Validate whether the system turns off when Max_Torque_Amplitude is exceeded within 50ms of fault tolerant.
Functional Safety Requirement 01-02	Set the value of Max_Torque_Frequency such that it is enough to warn the driver without causing steering loss.	Validate whether the system turns off when Max_Torque_Amplitude exceeds fault tolerant limits.

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional	Ensure that LKA torque is applied only for a	B	500 ms	Turn off LKA

Safety Requirement 02-01	limited time not more than Max_Duration			setting 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	Test if LKA is active until the Max_Duration is reached and post warning light turns on.	LKA is turned off when Max_Duration is reached

Refinement of the System Architecture

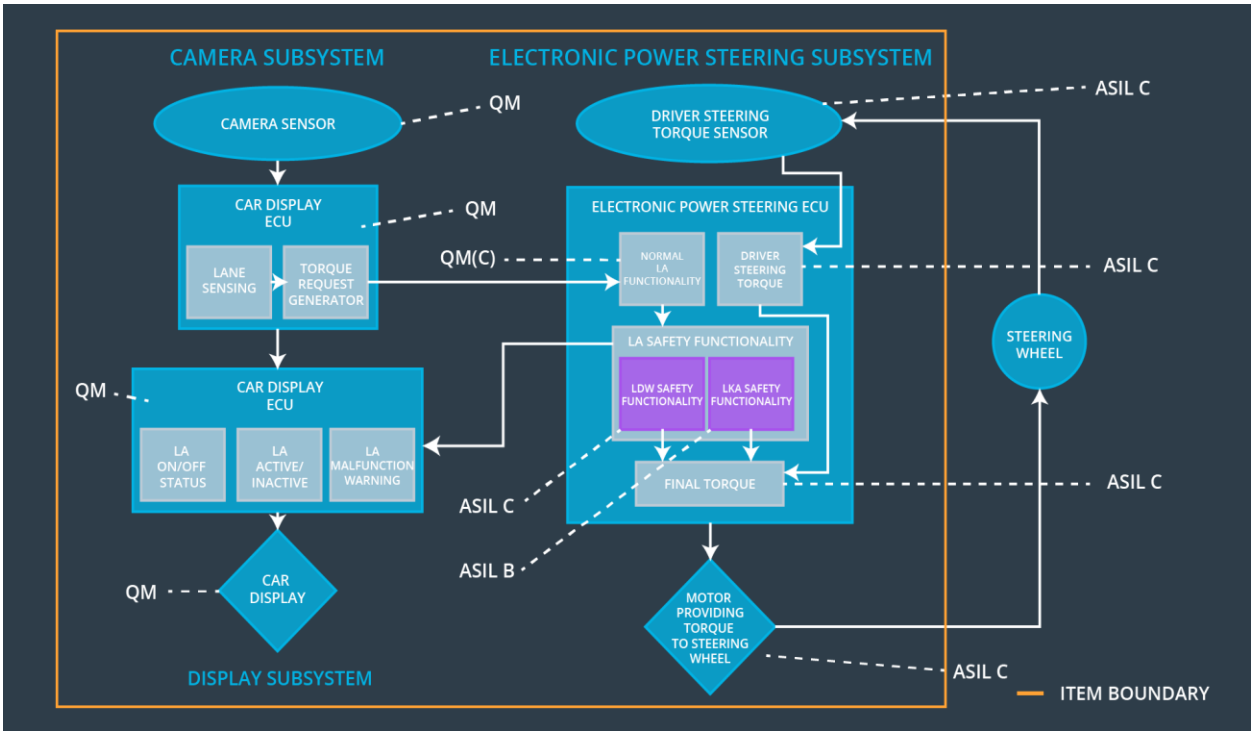

Figure 2System Architecture

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 Electronic Power Steering ECU shall ensure that the amplitude of Lane Departure Warning oscillating torque is below Max_Torque_Amplitude	**Responsible**	**Not Responsible**	**Not Responsible**
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the Frequency of Lane Departure Warning oscillating torque is below Max_Torque_Frequency	**Responsible**	**Not Responsible**	**Not Responsible**
Functional Safety Requirement 02-01	The Electronic Power Steering Shall ensure that the Lane Keeping Torque is applied for a maximum duration of Max_Duration	**Responsible**	**Not Responsible**	**Not Responsible**

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	Warning Light on Dashboard and warnings displayed on car display

WDC-02	Turn OFF the Functionality	Malfunction_03	Yes	Warning Light on Dashboard and warnings displayed on car display