Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
22-05-2018	1.0	Akshatha Holla	Functional Safety Concept

Table of Contents

Purpose of the Functional Safety Concept

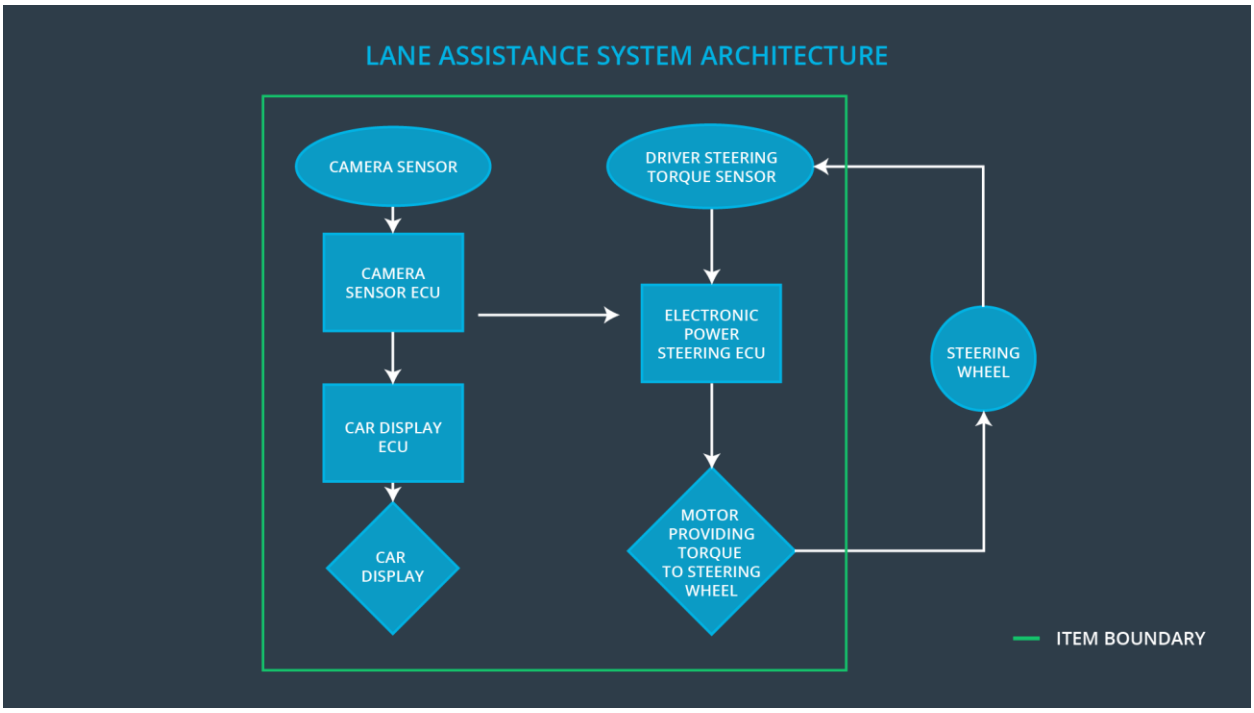
The purpose of functional safety is avoiding accidents by reducing risk to acceptable levels. In order to achieve this a functional safety concept document is created by identifying the elements and subsystems that can be used to meet the safety goals, then the safety goals are refined to functional safety requirements which are further allocated to relevant parts of item architecture. Then the system architecture is refined to handle the new requirements.

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 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.

Preliminary Architecture



The preliminary architecture of the Lane assistance system can be seen above.

Description of architecture elements

Element	Description
Camera Sensor	The camera sensor is used to capture images of the road and provides them as an input to the Camera sensor ECU.
Camera Sensor ECU	The Camera sensor ECU takes the input from the camera sensor and calculates the position of the car with respect to the lane lines that are detected by it.
Car Display	Provides visual warnings in cases of lane departure and other issues.
Car Display ECU	The car display ECU takes input from the Camera sensor ECU and processes the warnings to be provided to the car display.
Driver Steering Torque Sensor	Driver Steering Torque Sensor measures the amount of torque applied by the driver to the steering wheel.

Electronic Power Steering ECU	Takes the steering wheel torque input applied by the driver and the torque necessary to adjust the car to drive at the center of the expected lane from the camera ECU and provides appropriate input torque value to the motor.
Motor	Takes appropriate torque input from Electronic Power steering ECU and applies it to 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	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 (above limit)
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order	NO	The lane keeping assistance function is not limited in time duration which leads

	to stay in ego lane		to 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 oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Ensuring that the torque amplitude is below Max_Torque_Amplitude
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	Ensuring that the torque frequency is below Max_Torque_Frequency

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	The Max_Torque_Amplitude value should be a value that can be handled by the driver	Verify that when the torque amplitude crosses the Max_Torque_Amplitude limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.
Functional Safety Requirement 01-02	The Max_Torque_Frequency value should be a value that can be handled by the driver	Verify that when the torque frequency crosses the Max_Torque_Frequency limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval

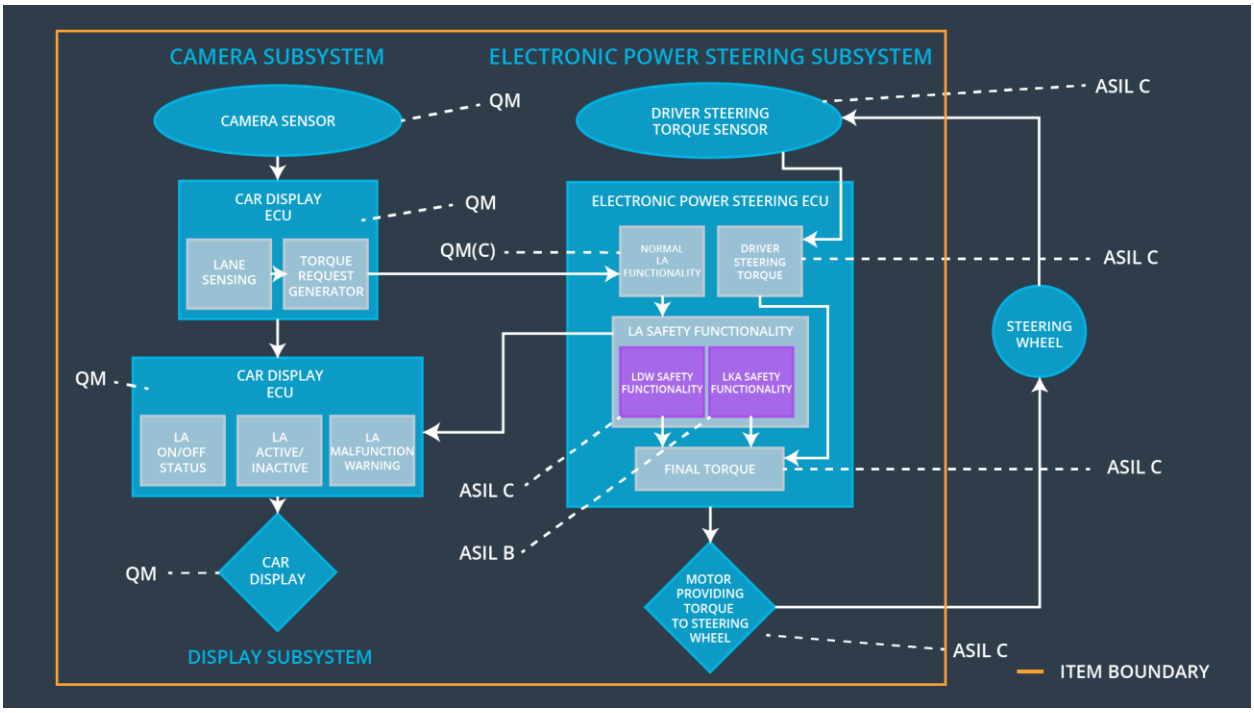
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The Lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving	B	500ms	Turn off the Lane keeping assistance function

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	The Max_duration should be a value which ensures that the driver does not take his hands off the wheel entirely	Test that the Lane keeping assistance turns off after Max_duration

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 Electronic Power Steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	**x**		
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	**x**		
Functional Safety	The electronic power steering ECU shall ensure that the lane	**x**		

Requirement 02-01	keeping assistance torque is applied for only Max_Duration			

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 departure Warning on car display
WDC-02	Turn off LKA functionality	Malfunction_03	Yes	LKA Warning on display