Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
25-05-2018	1.0	Harveen Singh	Initial Draft
26-05-2018	2.0	Harveen Singh	Finalized Version

Table of Contents

Purpose of the Functional Safety Concept

Functional Safety looks at the system from a higher level without diving into the technical details of the system. It looks at general functionality of the item. Goal here is to reduce the risks below the acceptable levels.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	Oscillating torque should be limited
Safety_Goal_02	Lane assistance system should be time limited

Preliminary Architecture

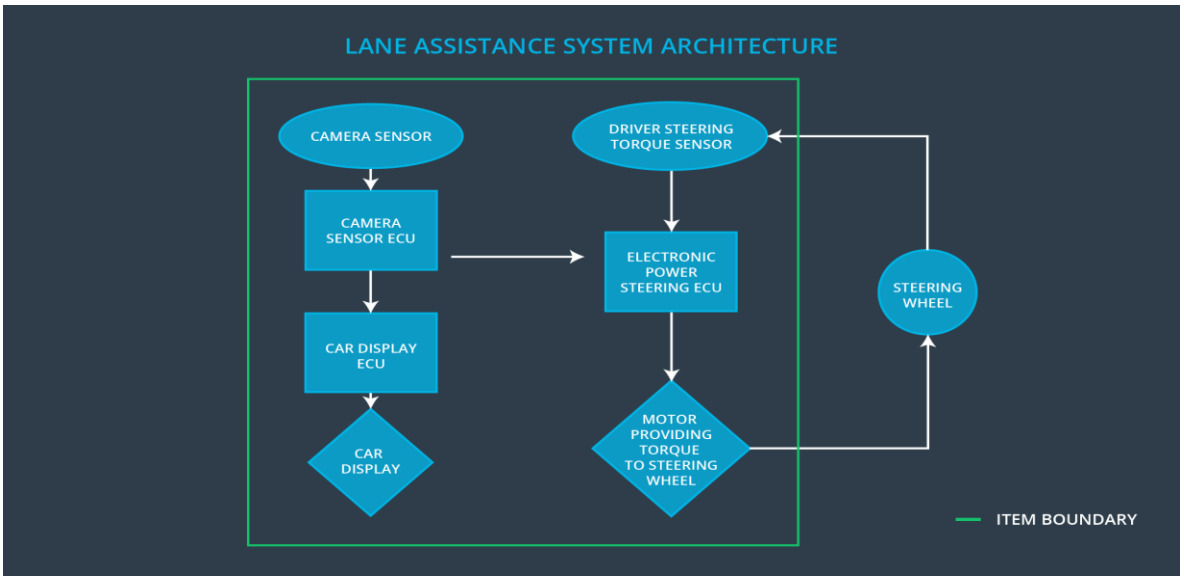

Fig 1. Lane Assistance System Architecture
[image source Udacity course content]

Description of architecture elements

Element	Description
Camera Sensor	Capture images and provide them to the camera sensor ECU continuously
Camera Sensor ECU	Detect Lane Lines and send the message when car has accidently departed the lane to Car display unit and Electronic Power Steering ECU
Car Display	Display the status of the systems and warnings when a system malfunction
Car Display ECU	It controls the things displayed on the car display in accordance with the inputs received from other systems.
Driver Steering Torque Sensor	It measures the torque applied to the steering wheel.
Electronic Power Steering ECU	It takes input from Driver Steering Torque Sensor and camera ECU and decides on the amount of torque needed to be applied on the steering wheel
Motor	The Motor is actuated by the input from Electronic Power Steering ECU. It applies the requisite torque 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 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.

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 Lane Departure Warning Torque Request 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	50 ms	Set Lane Departure Warning Torque Request 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	Value of Max_Torque_Amplitude is chosen such that it is adequate enough to warn the driver and low enough to not cause steering loss.	Validate whether the system turns off when Max_Torque_Amplitude is exceeded.
Functional Safety Requirement 01-02	Value of Max_Torque_Frequency is chosen such that it is adequate enough to warn the driver and low enough to not cause steering loss.	Validate whether the system turns off when Max_Torque_Frequency is exceeded.

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	Lane keeping assistance Function will be time limited for a Max_Duration	B	500ms	Set Lane Keeping Assistance oscillating torque amplitude 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	Value for max_duration chosen is large enough to bring back the vehicle to the center of the lane and small enough to discourage driver taking hands off the steering wheel	Verify that the LKA function turns off when the Max_Duration is exceeded

Refinement of the System Architecture

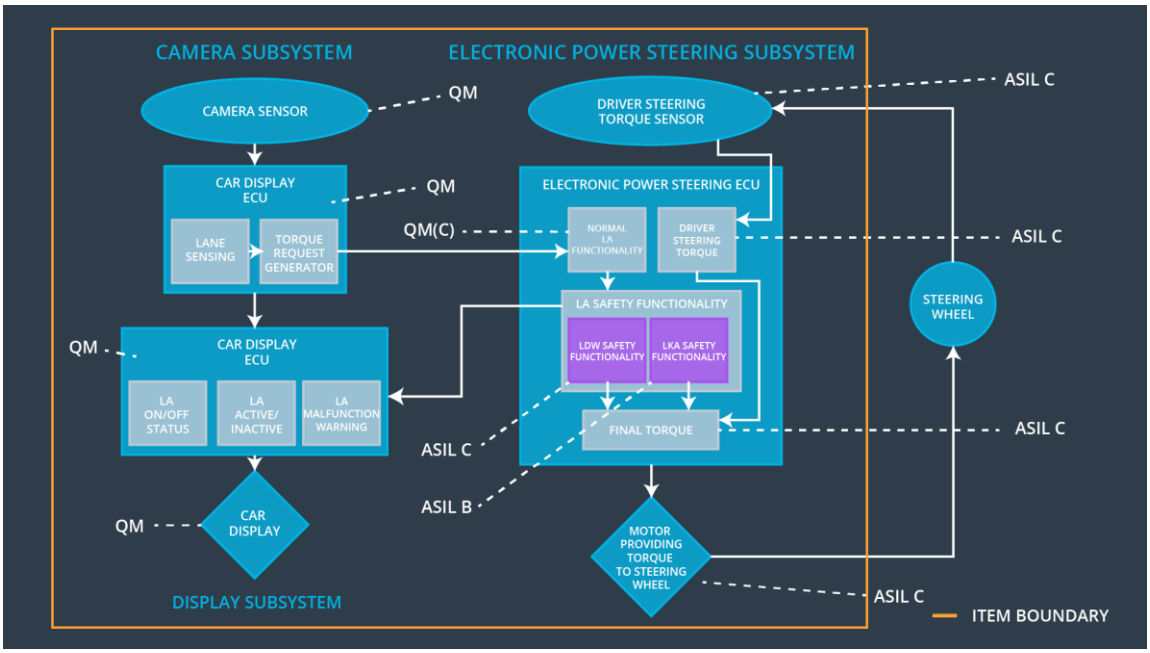

Fig 1. Lane Assistance System Architecture
[image source Udacity course content]

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