Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]
Template Version 1.0, Released on 2017-06-21

Document history

E2 - Low probability

Date	Version	Editor	Description

08/13/2017	1.0	Yuesong Xie	First Commit

Table of Contents

Contents

Purpose of the Functional Safety Concept

Allocates safety goals and functional safety requirements to the system architecture. It looks at the general functionality of the item and does not cover technical implementation.

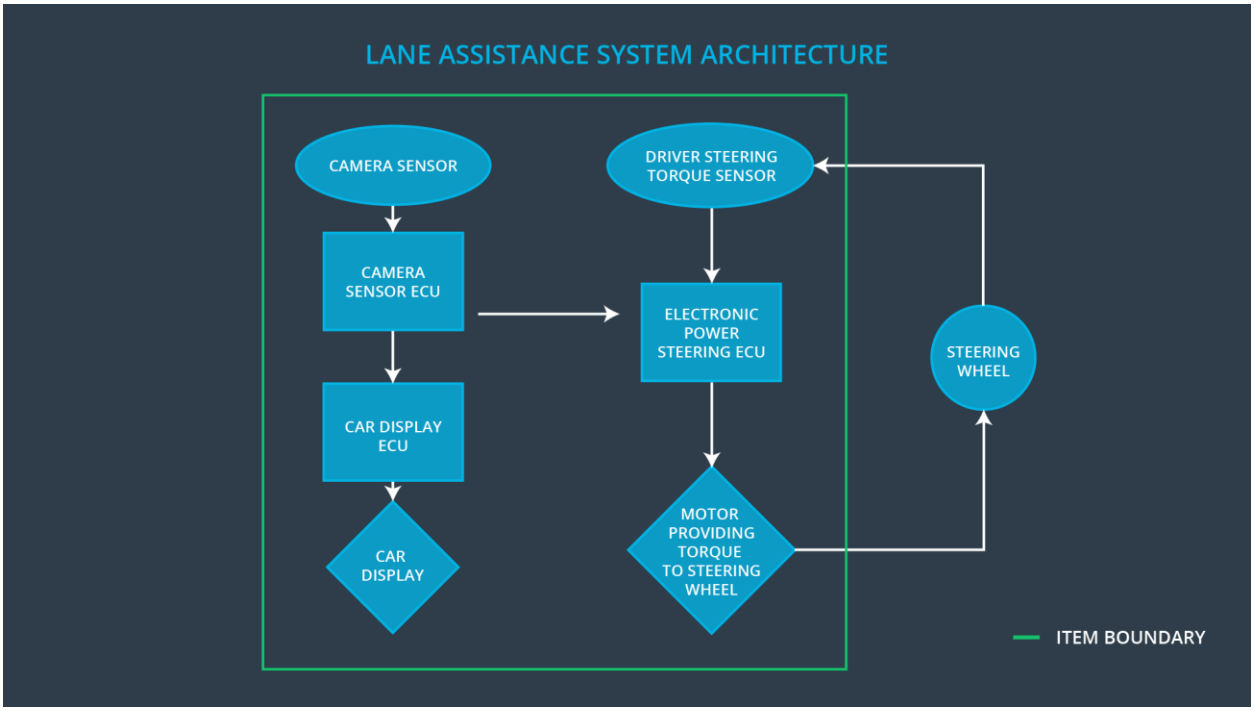
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal

Safety_Goal_01	The oscillating steering torque from the LDW function shall be limited
Safety_Goal_02	The LKA function shall be time limited and the additional steering torque shall end after a given time interval
Safety_Goal_03	The LKA function shall be deactivated during snowfall (degraded view) conditions
Safety_Goal_04	The LKA function shall be deactivated during heavy steering input by the driver

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Sends an image stream to the Camera Sensor ECU
Camera Sensor ECU	Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake
Car Display	Provides feedback to the driver about on/off and active/inactive status of the Lane Assistance system

Car Display ECU	Processes input from Camera Sensor ECU and engages/disengages LEDs on the Car Display
Driver Steering Torque Sensor	Responsible for measuring the torque provided by the driver
Electronic Power Steering ECU	Responsible for final steering torque output. Adds an appropriate amount of torque based on a Lane Assistance system torque request
Motor	Carries out the Electronic Power Steering ECU torque request and provides 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	NO	The lane keeping

	Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane		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 electronic power steering ECU shall ensure that the oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Off
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Off

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	Test how drivers react to different torque amplitudes to prove that we chose an appropriate value.	Software test: When the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that we chose an appropriate value.	Software test: When the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval

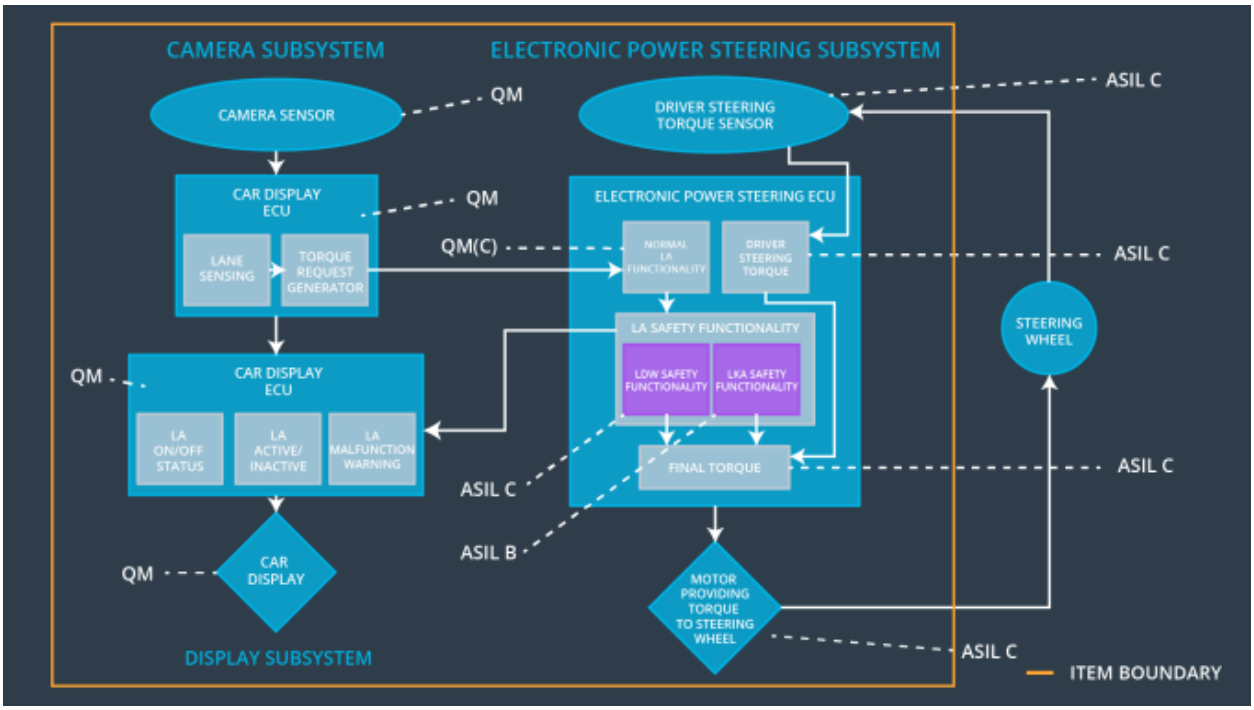
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	Off

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 that the max_duration chosen really does dissuade drivers from taking their hands off the wheel	Software Test: Verify that the system really does turn off if the lane keeping assistance every exceeded 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 oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the oscillating torque frequency is below Max_Torque_Frequency	**X**		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is	**X**		

	applied for only Max_Duration			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Off	Oscillating torque frequency is above Max_Torque_Amplitude or Max_Torque_Frequency	Yes	LED on Car Display
WDC-02	Off	Lane keeping assistance torque is applied for more than Max_Duration	Yes	LED on Car Display