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
24-May-2018	1.0	Nishant Katariya	Initial Draft

Table of Contents

Purpose of the Functional Safety Concept

The Main Purpose of the Functional Safety Concept is to derive functional safety requirement from the safety goals defined in HARA. To derive safety requirements Functional safety concept document identifies which sub systems actually responsible for the risk and relevant to safety goal. It documents system high level requirement these are allocated to different parts of the item which are then used to identify technical 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 LDW (Lane departure Warning) function shall be limited.
Safety_Goal_02	LKA (Lane Keeping Assistance)function shall be time limited and the additional steering torque shall end after a given timer period so that the driver cannot misuse the system for fully autonomous driving.

Preliminary Architecture

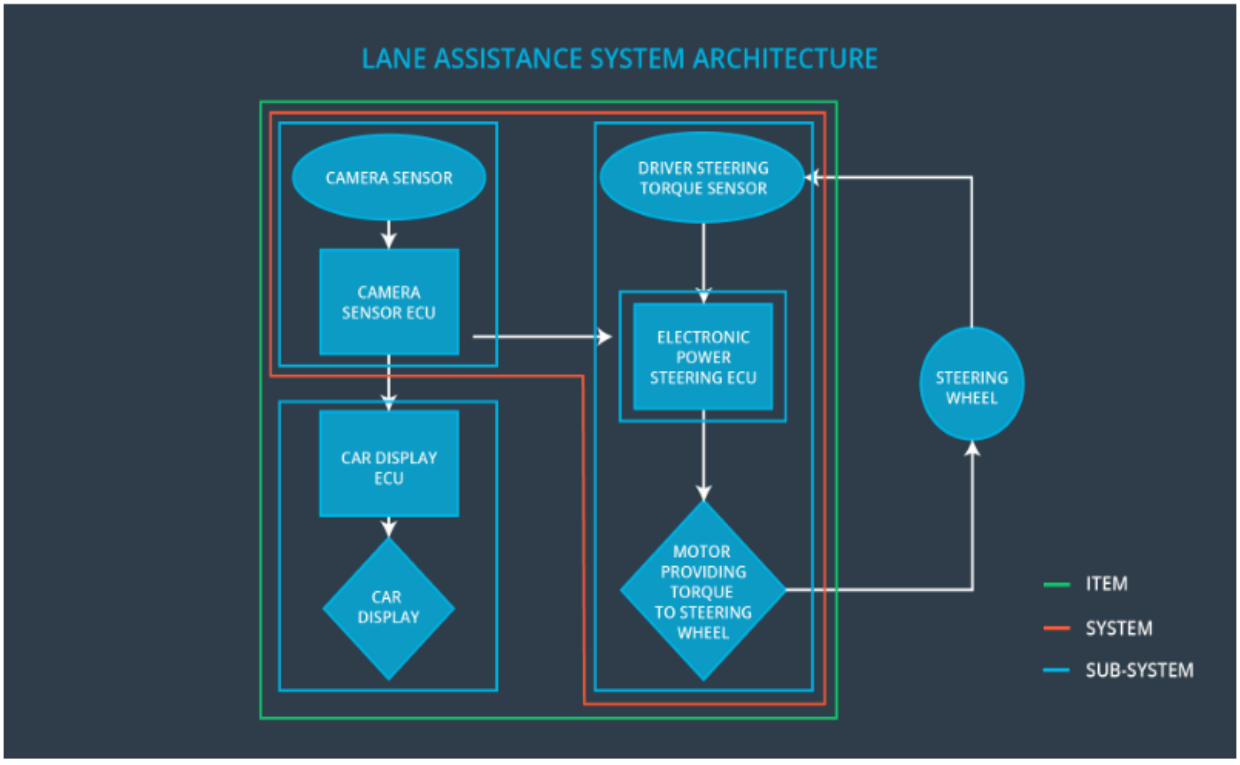


Fig 1.1

Description of architecture elements

Element	Description
Camera Sensor	Camera sensor perceives the vehicle leaving the lane; it sends the signal to the Electronic power steering system request to turn/vibrate the steering wheel. ECU (Electronic Control Unit) is a microcomputer that contains software and hardware specific to vehicle's functionality.
Camera Sensor ECU	The camera ECU have the hardware and software required for detecting lanes using computer vision techniques like machine learning or image processing.
Car Display	Displays the warning and status of the system on Display
Car Display ECU	ECU have the hardware and software required to display messages on Car display
Driver Steering Torque Sensor	It senses how much steering force is applied by the driver.
Electronic Power Steering ECU	It controls the Motor attached to Steering wheel
Motor	It is actuator to generate torque and rotate 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	MORE	Lane Departure

	Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback		Warning (LDW) function applies high oscillating steering torque amplitude(above limit) as feedback
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	Lane Departure Warning (LDW) function applies high oscillating steering torque with high frequency(above limit) as feedback
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 (LKA) function is not limited in time interval which lead to misuse as an fully autonomous driving system

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	Steering 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	Oscillation 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	Testing of drivers react to different torque amplitudes to determine appropriate value of Max_Torque is chosen.	Verification of system turning off when LDW exceeds Max_Torque
Functional Safety Requirement 01-02	Testing of drivers react to different torque Frequencies to determine appropriate value of Max_Torque_Frequency is choosen.	Verification of system turning off when LDW exceeds Max_Torque_Frequency

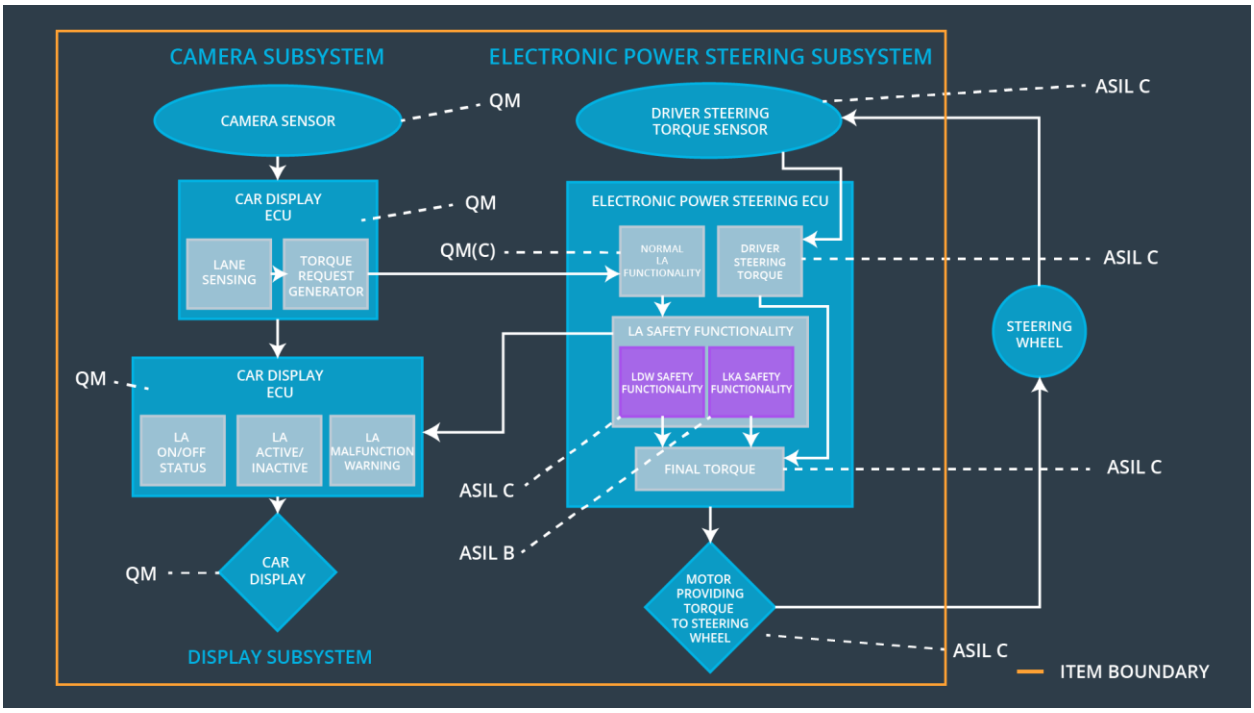
Lane Keeping Assistance (LKA) Requirements:

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	Lane Assistance Functionality is 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	Validate Max_Duration really assures that driver will keep hands on steering wheel and will not consider system as fully autonomous	Verification of system turning off when LKA exceeds 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	**X**		
Functional Safety Requirement 02-01	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn Off LDW functionality	Malfunction_01	Yes	LDW malfunction warning on Car display
WDC-02	Turn Off LDW functionality	Malfunction_02	Yes	LDW malfunction warning on Car display
WDC-03	Turn Off LKA functionality	Malfunction_03	Yes	LKA malfunction warning on Car display