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
6/2/2018	1.0	Ruiuxan.li	First release

Table of Contents

Purpose of the Functional Safety Concept

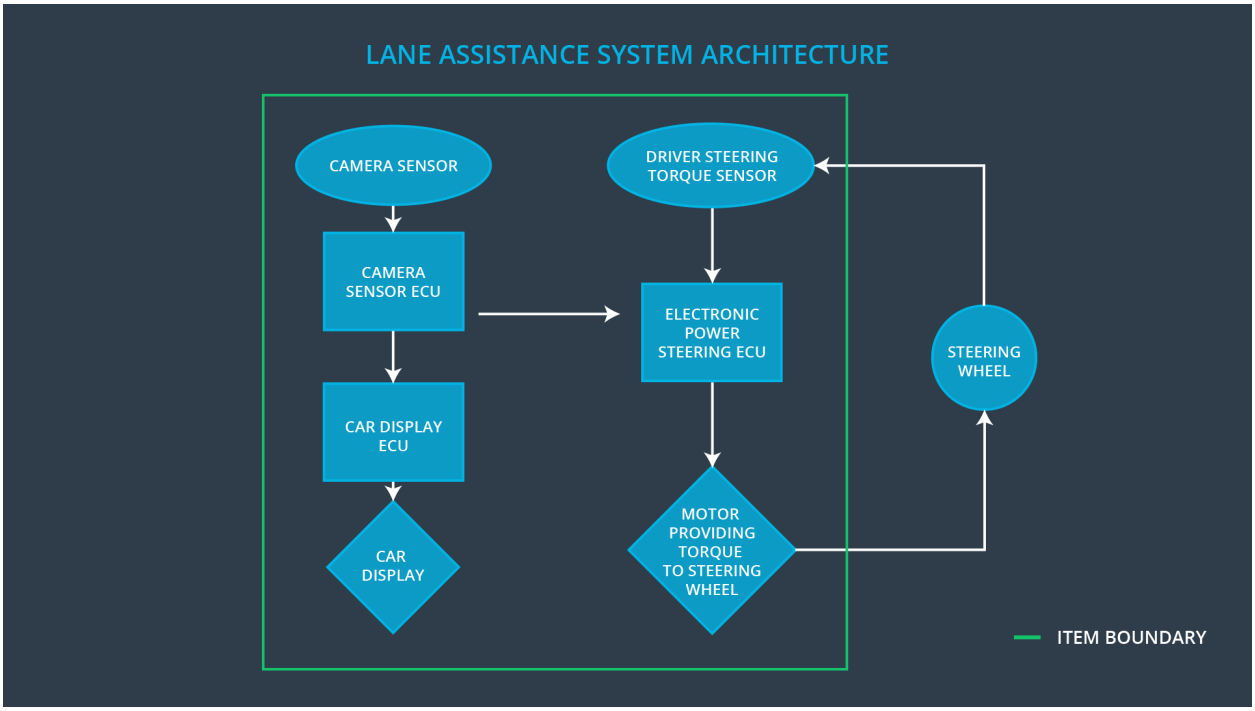
The purpose of functional safety concept is to identify which subsystems and elements can be used to meet safety goals, and allocates functional safety requirements to the relevant parts in the system architecture. Allocation could involve expanding the system architecture with new element blocks.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating torque to the steering wheel from the lane departure warnin 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



Description of architecture elements

Element	Description
Camera Sensor	The camera sensor reads in images from the road.
Camera Sensor ECU	The camera sensor ECU identifies when the vehicle has accidentally departed its lane. And sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	Graphic interface used to display the warning messages and setting changes.
Car Display ECU	Processes input from camera subsystem and display the messages on the Car Display
Driver Steering Torque Sensor	Responsible for measuring the torque applied by the driver
Electronic Power Steering ECU	Vibrates the steering wheel when vehicle is drifting away from the current lane unintentionally. Add appropriate amount of torque based on feedback from torque sensor to keep vehicle in current lane.
Motor	Actuator used to apply requested torque to 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	The lane departure

	Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback		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 electronic power steering subsystem shall ensure that the oscillating torque amplitude is less than Max_Torque_Amplitude	C	50ms	LDW torque output is set to zero
Functional	The electronic power steering subsystem	C	50ms	LDW torque

Safety Requirement 01-02	shall ensure that the oscillating torque frequency is less than Max_Torque_Frequency			output is set 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	Test how drivers react to different torque amplitudes to prove that we chose an appropriate value	Verify that 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	Verify that 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:

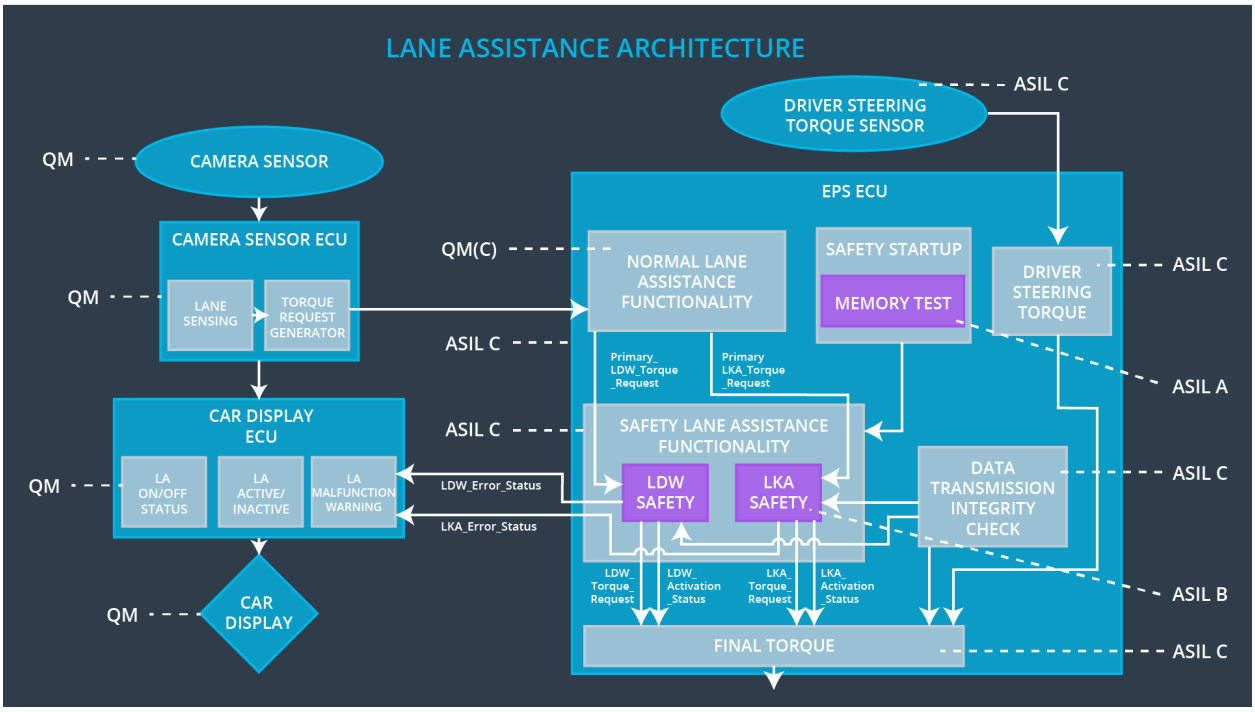
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	Verify that when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval	B	500	off

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement	Validate that the Max_Duration chosen really did dissuade drivers from taking their hands off the wheel	Verify that the system really does turn off if the lane keeping assistance every exceeded MAX_DURATION

02-01		

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	The electronic power steering ECU shall ensure that the	**X**		

Requirement 01-02	oscillating torque amplitude is below Max_Torque_Frequency			
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	**X**		

Warning and Degradation Concept

[Instructions: Fill in the warning and degradation concept.]

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