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
04 Sep 2017	1.0	Navneet Latawa	First submission

Table of Contents

Purpose of the Functional Safety Concept

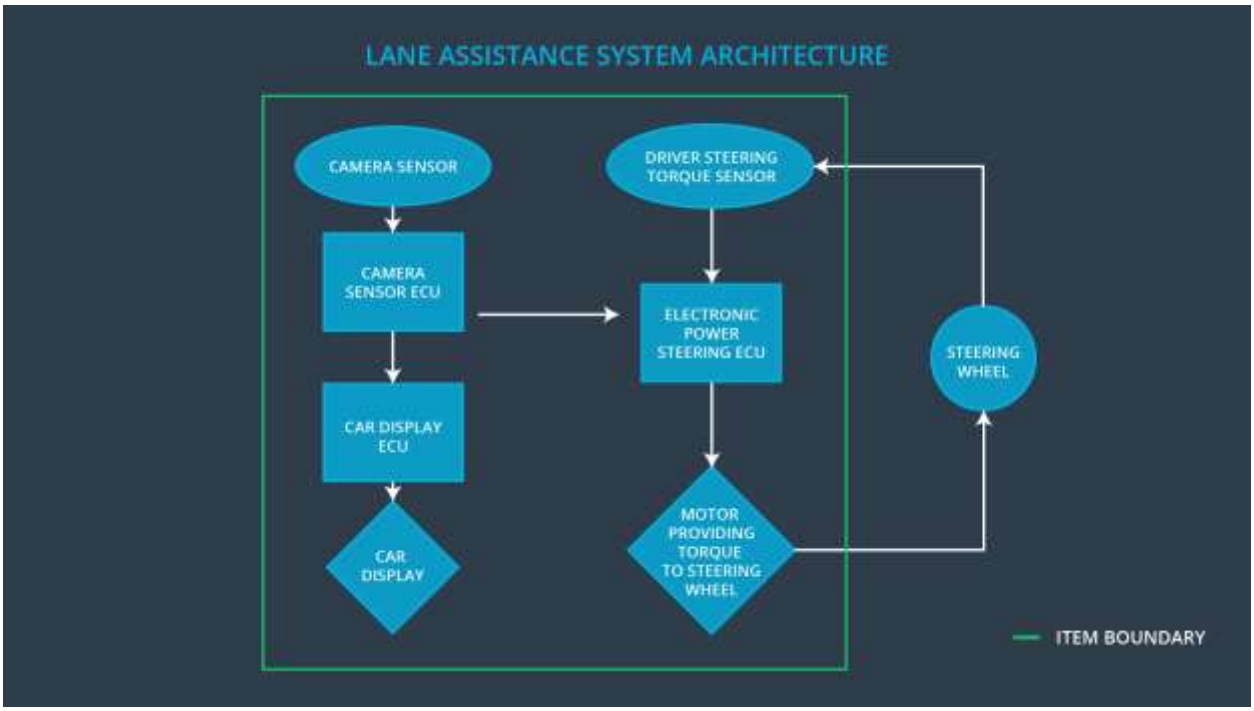
The purpose of Functional Safety Concept is to avoid accidents by reducing risk to the acceptable levels. Identifying risks of each subsystems and then identifying relevant subsystems needed to meet the safety goals constitute Functional Safety Concept. Functional Safety concept document is prepared to identify Safety goals, high level safety requirements to meet these goals and assign these requirements to proper subsystems in the architecture diagram.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The Lane Keeping Assistance function will be time limited so that the additional torque will be applied for only a short time.
Safety_Goal_02	The Lane Departure Warning function shall apply an oscillating steering torque limited in magnitude and frequency to provide the driver a haptic feedback.
Safety_Goal_03	The Lane Keeping Assistance function should be deactivated if the sensors are not working.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Camera sensor will help in detecting lane lines
Camera Sensor ECU	The Electronic control unit determines how much extra torque to apply when the vehicle leaves lane by mistake.
Car Display	The Display element which displays any warning signs.
Car Display ECU	The electronic control unit for car display which sends signals to the display
Driver Steering Torque Sensor	This sensor determines how much torque is manually applied by the driver.
Electronic Power Steering ECU	This Electronic control unit combines camera sensor torque and driver applied torque and sends the combined torque signal value to the motor.
Motor	This applies the torque value sent by EPS ECU to the steering.

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	LDW function provided oscillating steering of **magnitude** more than the limit.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	More	LDW function provided oscillating steering of **frequency** more than the 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
Malfunction_04	Lane Departure Warning (LDW) function shall apply an oscillating	Late	LDW function was late in providing isolating steering torque.

	steering torque to provide the driver a haptic feedback		
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	Late	LKA function was late in providing isolating steering torque.

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 lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	The electronic power steering ECU reduces the oscillating torque amplitude to zero.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50ms	The electronic power steering ECU reduces the oscillating torque 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	Validate that the Max_Torque_Amplitude is the correct value beyond which it is difficult to control for an average driver.	Verify that the ECU sets Torque to zero if the torque amplitude is higher than Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate that the Max_Torque_Frquency is the correct value beyond which it is difficult to control for an average driver.	Verify that the ECU sets Torque to zero if the torque frequency is higher than Max_Torque_Frequency.

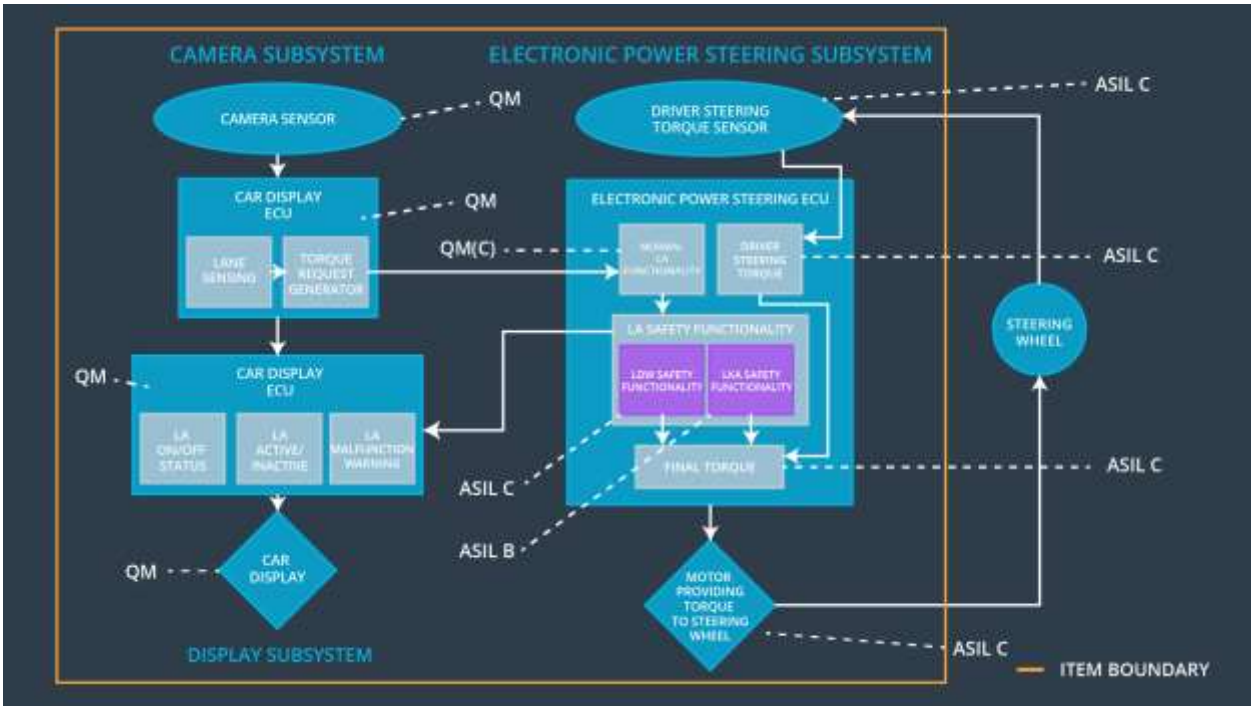
Lane Keeping Assistance (LKA) Requirements:

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	The electronic power steering ECU reduces the oscillating torque 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	Validate that the time (Max_Duration) identified is the correct time to make sure that driver does not consider the car as a fully autonomous vehicle.	Verify that the torque is set to zero if ECU determines that the extra torque is applied for more than the 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 Requirement 01-03	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the LDW functionality.	LDW functionality has applied the torque of high magnitude or high frequency.	Yes	Warning on Display.
WDC-02	Turn off the LKA functionality.	LKA functionality is always on.	Yes	Warning on Display.