Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 2.0

Document history

Date	Version	Editor	Description
01/03/2019	1.0	Chris Sketch	Initial Documentation
01/05/2019	2.0	Chris	Add Functional Safety Concept 01-03

Table of Contents

Purpose of the Functional Safety Concept

The purpose of the functional safety concept is to avoid accidents by reducing risk to acceptable levels.

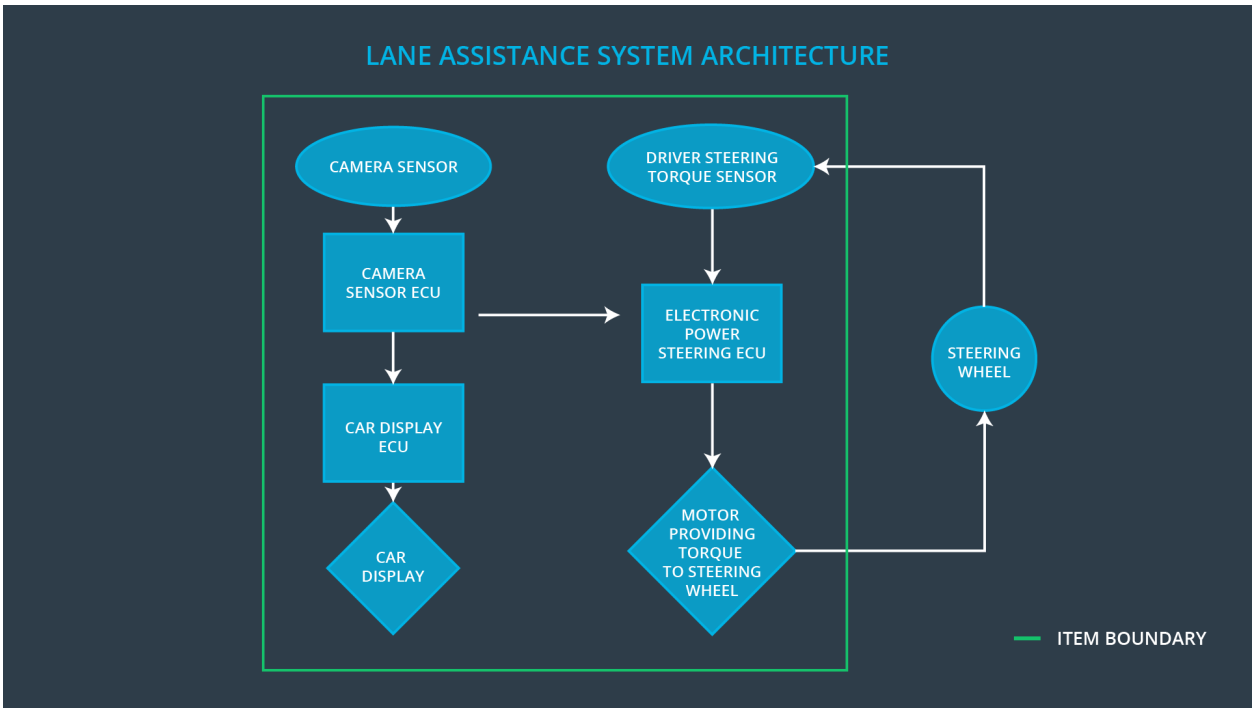
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

The lane assistance item is composed of two functions: lane departure warning and lane keeping assistance. The lane departure warning function has one goal and the lane keeping function has two goals.

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the lane departure warning 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
Safety_Goal_03	The lane keeping assistance function's car display subsystem shall reliably display the lane keeping assistance indicator.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Senses visual information in the environment such as the lane markings and geometry of the road so that the lane assitance item can determine its lane and its position within the lane.
Camera Sensor ECU	Processes information received from the camera sensor to determine the current lane and the vehicles position in the lane. Sends requests to the car display ECU and the

	electronic power steering ECU.
Car Display	Displays an icon to the driver to indicate that the vehicle is departing the lane or the lane keeping function is activated
Car Display ECU	Receives request from the camera sensor ECU and turns on the car display.
Driver Steering Torque Sensor	Senses the torque that is being applied to the steering wheel. The sensor is necessary to steer and add torque in a controlled manner.
Electronic Power Steering ECU	Receives information from the driver steering torque sensor. Receives lane departure warning requests from the camera sensor ECU when the vehicle is departing the lane. Receives lane keeping assistance requests from the camera sensor ECU with information about the road geometry and the position of the vehicle on the road. Processes lane departure warning requests and determines the amount of torque to apply to the steering wheel. Processes lane keeping assistance requests to determine the amount of torque necessary to steer the vehicle to the center of the lane. Activates the motor providing torque to the steering wheel in order to oscillate the steering wheel. Activates the motor providing torque to the steering wheel in order to steer to the center of the lane
Motor providing torque to the steering wheel	Provides torque to the steering wheel in order to alert the driver that they are exiting the lane Provides torque to the steering wheel in order to steer the vehicle to the center of the lane

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 frequency (above limit)
Malfunction_03	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	LESS	The lane departure warning function applies an oscillating torque with very low frequency (below limit)
Malfunction_04	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	The electronic power steering ECU shall	C	50 ms	Lane departure torque is set to 0.

Requirement 01-01	ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude			
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Lane departure torque is set to 0.
01-03	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is above Min_Torque_Frequency	B	50 ms	Lane departure torque is set to 0.

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	Using a representative sample size of drivers, test that the value of Max_Torque_Limit is not too high to be uncontrollable or too low to be unnoticed	Test that after torque has exceeded Max_Torque_Limit that the lane departure warning output torque is set to 0 within the FTTI specified above.
Functional Safety Requirement 01-02	Using a representative sample size of drivers, test that the value of Max_Frequency_Limit is not too high to be uncontrollable or uncomfortable and not too low to be unnoticed or cause significant vehicle drift	Test that after torque has exceeded Max_Frequency_Limit that the lane departure warning output torque is set to 0 within the FTTI specified above.
Functional Safety Requirement 01-03	Using a representative sample size of drivers, test that the value of Min_Frequency_Limit is not too low to cause significant vehicle drift into other lanes	Test that after torque has dropped below Min_Frequency_Limit that the lane departure warning output torque is set to 0 within the FTTI specified above.

Lane Keeping Assistance (LKA) Requirements:

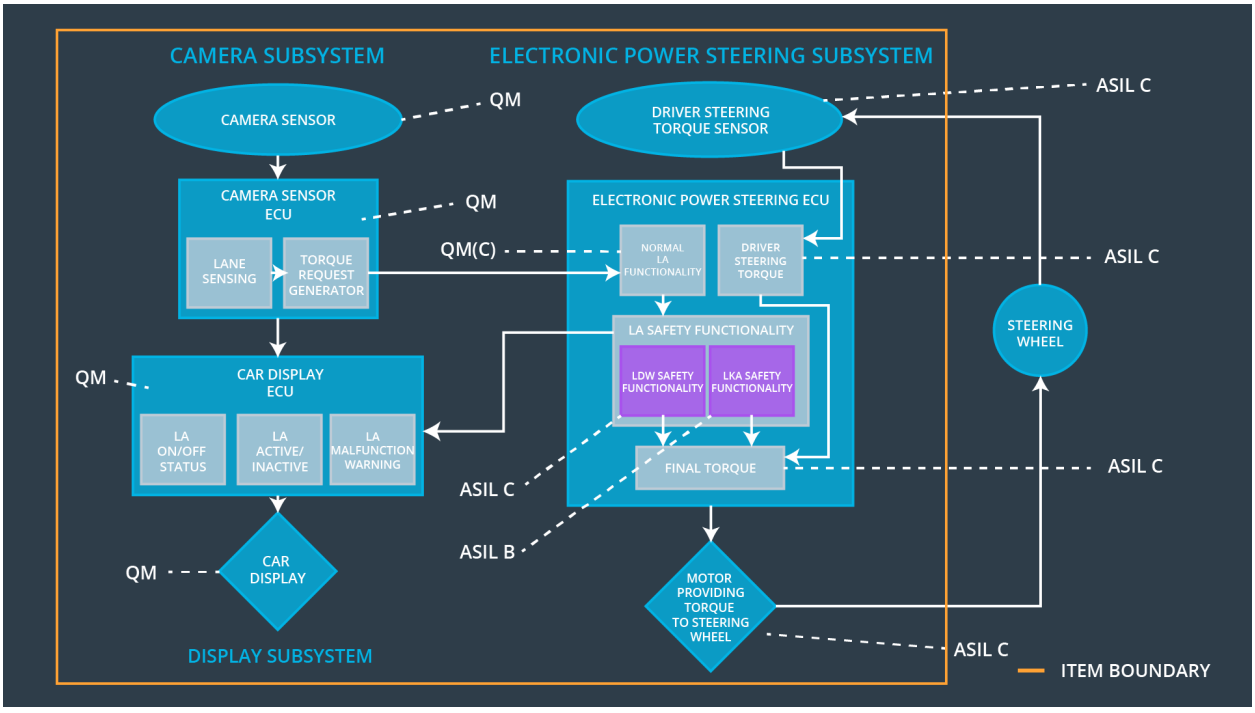
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State

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	500 ms	Lane assitance torque is set to 0.

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	Using a representative sample size of drivers, test that the value of Max_Duration discouraged drivers from shifting their attention away from the road	Test that after the lane assistance torque has been applied for Max_Duration, lane assistance torque is set to 0 within the FTTI specified above.

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic	Camera	Car Display

		Power Steering ECU	ECU	ECU
Functional Safety Requirement 01-01	The electronic power steering ECU shall ensure that the lane departure warning 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 warning oscillating torque frequncy 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 applied for only Max_Duration	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Driver Warning
WDC-01	Lane departure warning function turned off	Oscillating torque amplitude exceeds Max_Torque_Limit or oscillating torque frequency exceeds Max_Torque_Frequency or oscillating torque frequency drops below Min_Torque_Frequency	Car display shows message that lane departure warning is not available
WDC-02	Lane keep assistance function	Lane keeping assistance torque is applied for greater than Max_Duration	Car display shows message that lane keep assistance function is not available