Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
06/04/2019	1.0	Jian Li	Initial version

Table of Contents

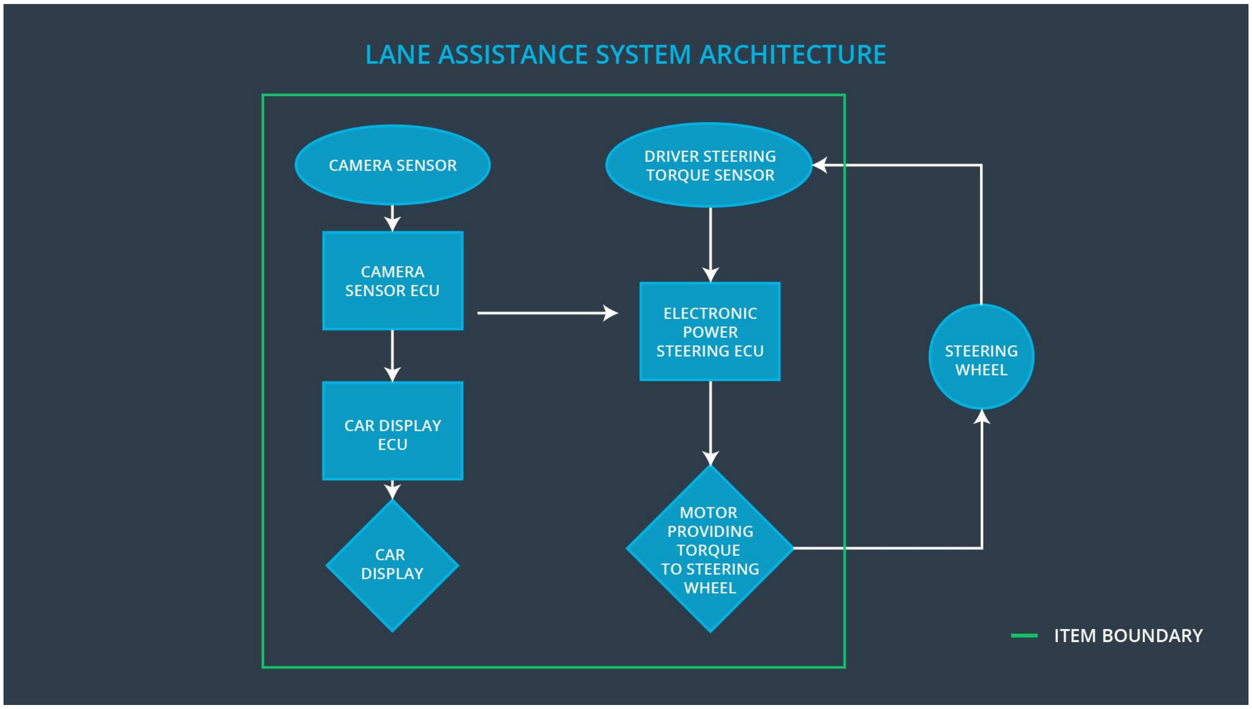
Purpose of the Functional Safety Concept

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 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.

Preliminary Architecture


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

Description of architecture elements

Element	Description

Camera Sensor	The Camera Sensor reads the 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 electronic power steering ECU.
Car Display	The Car Display shows the status of the function to the driver.
Car Display ECU	The Car Display ECU controls the Car Display based on the request to show warning on/off.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor measures the torque provided the driver.
Electronic Power Steering ECU	The Electronic Power Steering ECU reads the measured torque from the sensor and controls the Motor to add an appropriate amount of torque based on a torque request.
Motor	The Motor executes the request from Electronic Power Steering ECU and add an appropriate amount of 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	MORE	The lane departure warning function applies an oscillating torque with very high

	torque to provide the driver a haptic feedback		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 departure warning function applies an oscillating torque with very high torque frequency (above limit).

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	Turn off LDW
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	Turn off LDW

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional	Set the oscillating torque amplitude to	When the torque amplitude crosses

Safety Requirement 01-01	Max_Torque_Amplitude, and the warning light is ON.	the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.
Functional Safety Requirement 01-02	Set the oscillating torque amplitude to Max_Torque_Frequency, and the warning light is ON.	When the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

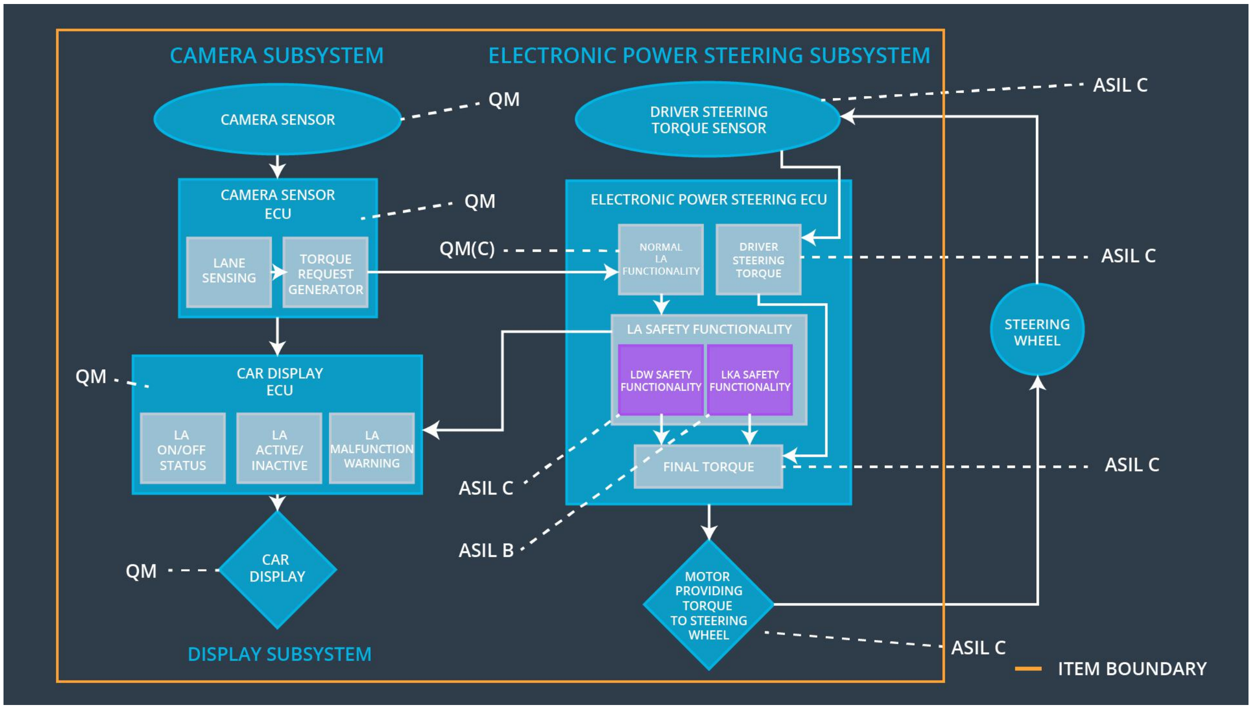
Lane Keeping Assistance (LKA) Requirements:

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	Turn off LKA

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	The max_duration chosen really did dissuade drivers from taking their hands off the wheel.	The system turns off when 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	x		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure 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 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 function	Torque crosses the Max_Torque	Yes	The warning light is on.
WDC-02	Turn off the function	Activated time elapsed over Max_Duration	Yes	The warning light is on.