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
11/21/2018	1.0	Claris Li	First draft

Table of Contents

Purpose of the Functional Safety Concept

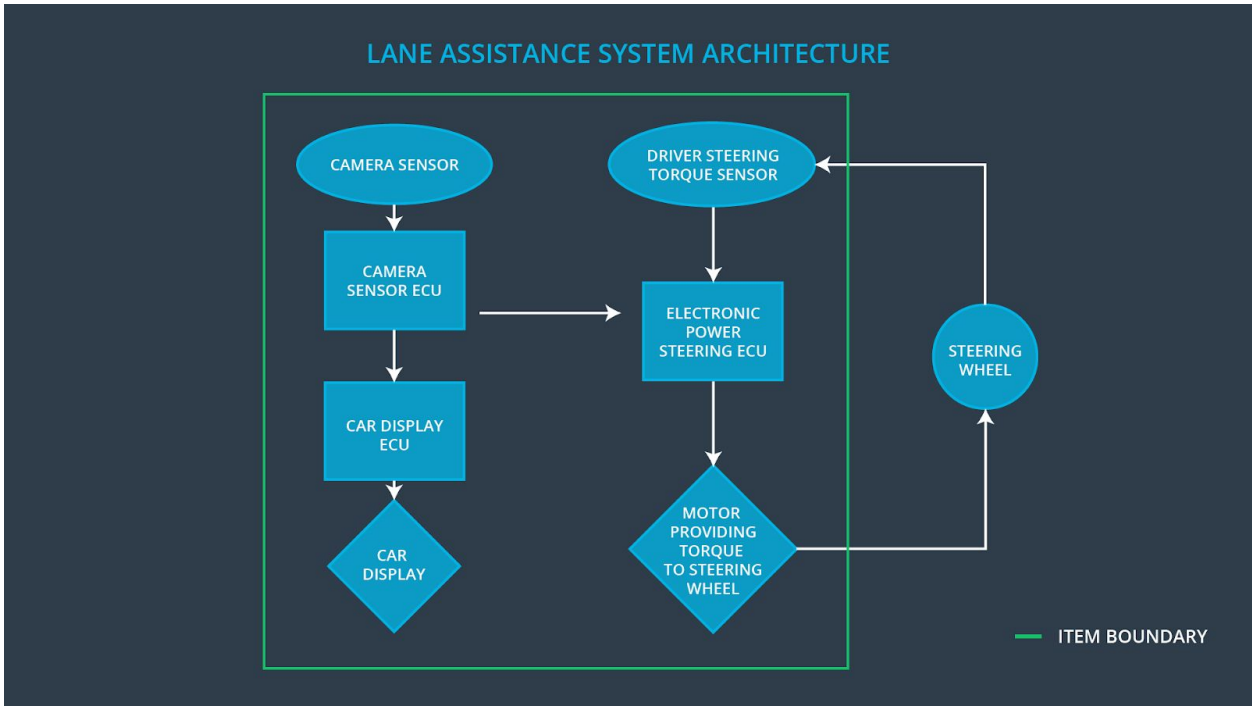
Defines a system architecture to ensure safety goals.

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 Lane Departure Warning function shall be limited.
Safety_Goal_02	The Lane Keeping Assistance function shall be time-limited, and additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.
Safety_Goal_03	The Lane Keeping Assistance function shall be deactivated when the camera sensor detects snow-covered road.
Safety_Goal_04	The LDW function shall be deactivated when the camera sensor cannot correctly detect the lanes, and it shall notify the driver when it's off.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Take pictures and send them to the camera sensor ECU
Camera Sensor ECU	Analyze the input images to detect lane departures, tell the steering wheel how hard to turn, and tell the car display to show the warning.
Car Display	Provide visual feedback to the driver to display warnings
Car Display ECU	Control the car display to show the warning as requested by the camera sensor ECU
Driver Steering Torque Sensor	Detect the amount of torque been applied by the driver
Electronic Power Steering ECU	Request the motor to vibrate or turn according to the request from the camera sensor ECU and how

	much the driver is already turning
Motor	Apply extra torque to the steering wheel as requested by the Electronic Power Steering ECU

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 torque frequency (above limit)
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply	NO	The lane keeping assistance function is not limited in time

	the steering torque when active in order to stay in ego lane		duration which leads to misuse as an autonomous driving function.
Malfunction_04	Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	The LKA function is not turned off when there's snow on road.
Malfunction_05	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	NO	The LDW function is not turned off when the camera sensor is not working.

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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	LDW is off
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	LDW is off

Functional Safety Requirement 01-03	The Lane Departure Warning item shall ensure that there's no lane departure oscillating torque when the camera sensor is not working.	A	500 ms	LDW is off

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 the Max_Torque_Amplitude chosen is neither too high for a driver to handle nor too low that the driver cannot feel the vibration.	Verify the Lane Departure Warning vibrates the steering wheel under Max_Torque_Amplitude
Functional Safety Requirement 01-02	Validate the Max_Torque_Frequency chosen is neither too high for a driver to handle nor too low that the driver cannot feel the vibration.	Verify the Lane Departure Warning vibrates the steering wheel under Max_Torque_Frequency
Functional Safety Requirement 01-03	Validate turning off the LDW function when the camera is not working is appropriate.	Verify the LDW is off when the camera is not working

Lane Keeping Assistance (LKA) Requirements:

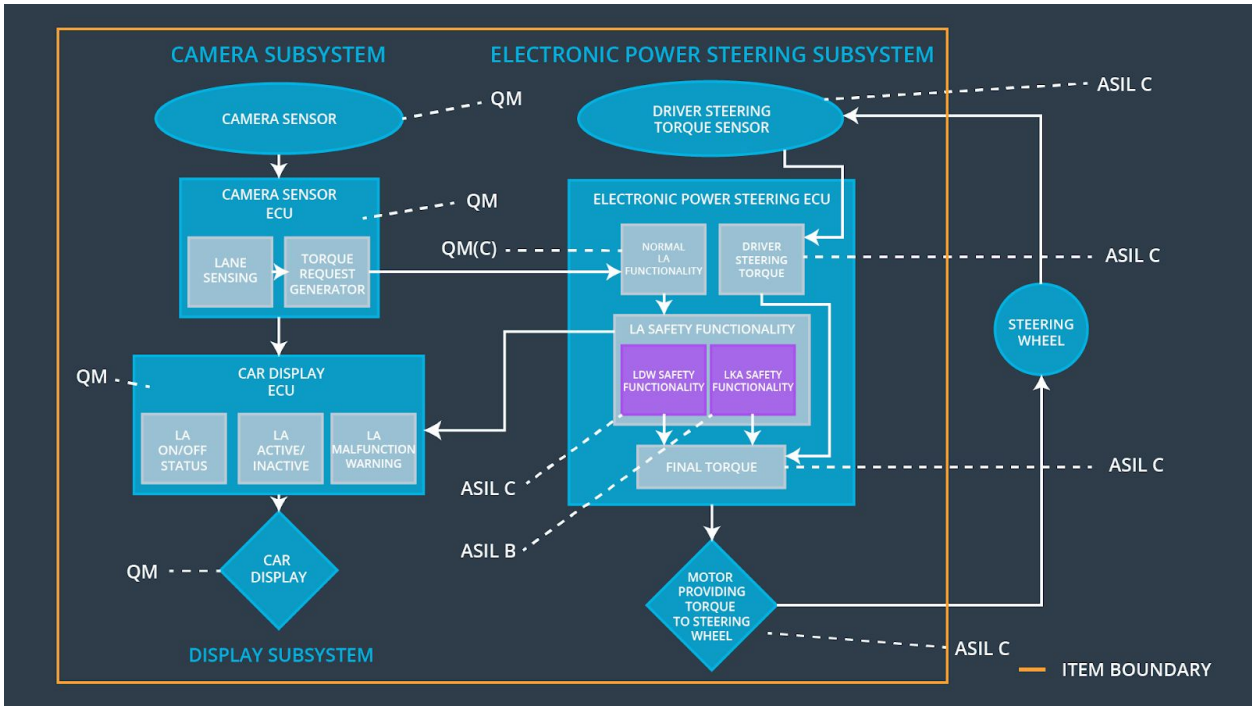
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requiremen	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	No extra torque applied after Max_Duration.

t 02-01				
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is deactivated when the camera detects snow-covered road with a confidence over Min_Snow_Confidence.	A	500 ms	No extra torque applied when there's snow on road.

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 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 ever exceeded Max_Duration
Functional Safety Requirement 02-02	Validate that the Min_Snow_Confidence chosen can reasonably identify the snow on the slippery road.	Verify that the system really does turn off if the camera detects snow on the road with a confidence over Min_Snow_Confidence.

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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below	**X**		

01-02	Max_Torque_Frequency.			
Functional Safety Requirement 01-03	The Lane Departure Warning item shall ensure that there's no lane departure oscillating torque when the camera sensor is not working.	**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**		
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is deactivated when the camera detects snow-covered road with a confidence over Min_Snow_Confidence.	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn the LDW off	Malfunction_01, Malfunction_02, Malfunction_05	Yes	Show the LDW Malfunction Warning on Car Display
WDC-02	Turn the LKA off	Malfunction_03, Malfunction_04	Yes	Show the LKA Malfunction Warning on

				Car Display