Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
11/2/17	1.0	Avnit Mackin	First attempt

Table of Contents

Purpose of the Functional Safety Concept

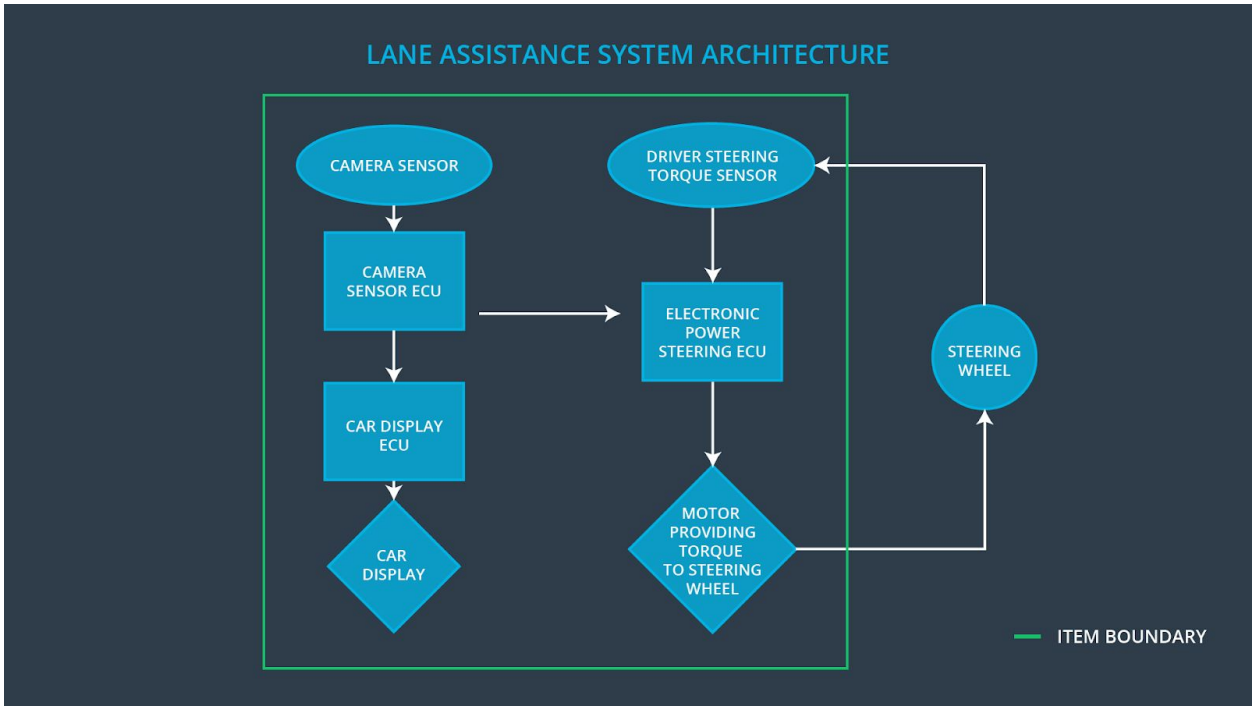
The functional safety concept identify the safety requirements and allocate these requirements to system diagrams. The functional safety concept looks at the general functionality of the system's items.

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 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



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 accidently departed its lane and sends the appropriate messages to Car Display ECU and the Electronic Power Steering ECU.
Car Display	The Car Display displays the lane assistance status to the driver (On/Off/Active/Inactive).
Car Display ECU	The Car Display display ECU sends the appropriate lane assistance status messages to Car Display.
Driver Steering Torque Sensor	Detect the driver steering torque.
Electronic Power Steering ECU	Gives the final Electronic Power Steering torque output.
Motor	Provides 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)	MORE	The lane departure warning function

	function shall apply an oscillating steering torque to provide the driver a haptic feedback		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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Set vibration torque to 0.
Functional Safety	The lane keeping item shall ensure that the lane departure oscillating torque	C	50 ms	Set vibration torque to 0.

Requirement 01-02	frequency is below Max_Torque_Frequency			

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.	Criteria : when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. Method: A software test inserting a fault into the system and seeing what happens.
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that we chose an appropriate value.	Criteria : when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. Method: A software test inserting a fault into the system and seeing what happens.

Lane Keeping Assistance (LKA) Requirements:

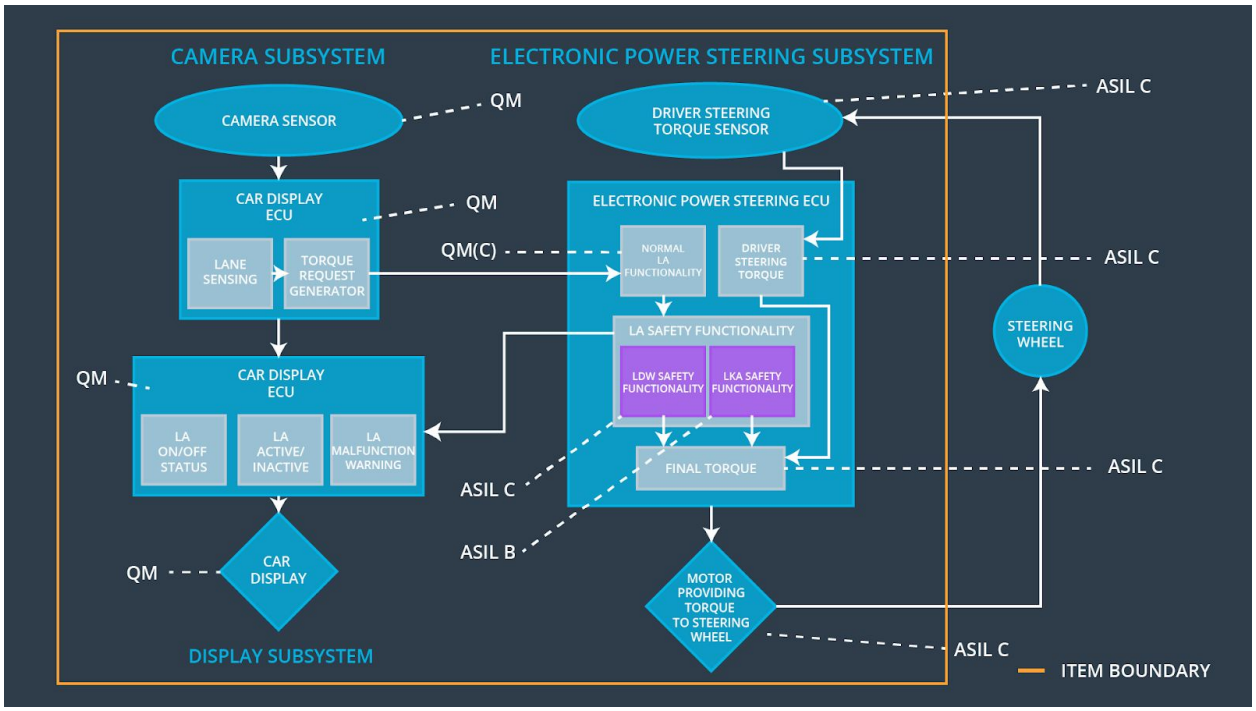
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional	The electronic power steering ECU shall	B	500 ms	The system will

Safety Requirement 02-01	ensure that the lane keeping assistance torque is applied for only Max_Duration			be turn off.

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.	Criteria : the system turn off if the lane keeping assistance every exceeded max_duration. Method: A software test inserting a fault into the system and seeing what happens.

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

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the functionality.	The lane departure oscillating	Yes	Yes - turn on a warning light.

		torque amplitude is equal/above Max_Torque_Amplitude or equal/above Max_Torque_Frequency		
WDC-02	Turn off the functionality.	The lane keeping assistance torque duration is equal or above Max_Duration	Yes	Yes - turn on a warning light.