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
21.12.2018	1.0	Usman Ijaz Malik	First Attempt

Table of Contents

Purpose of the Functional Safety Concept

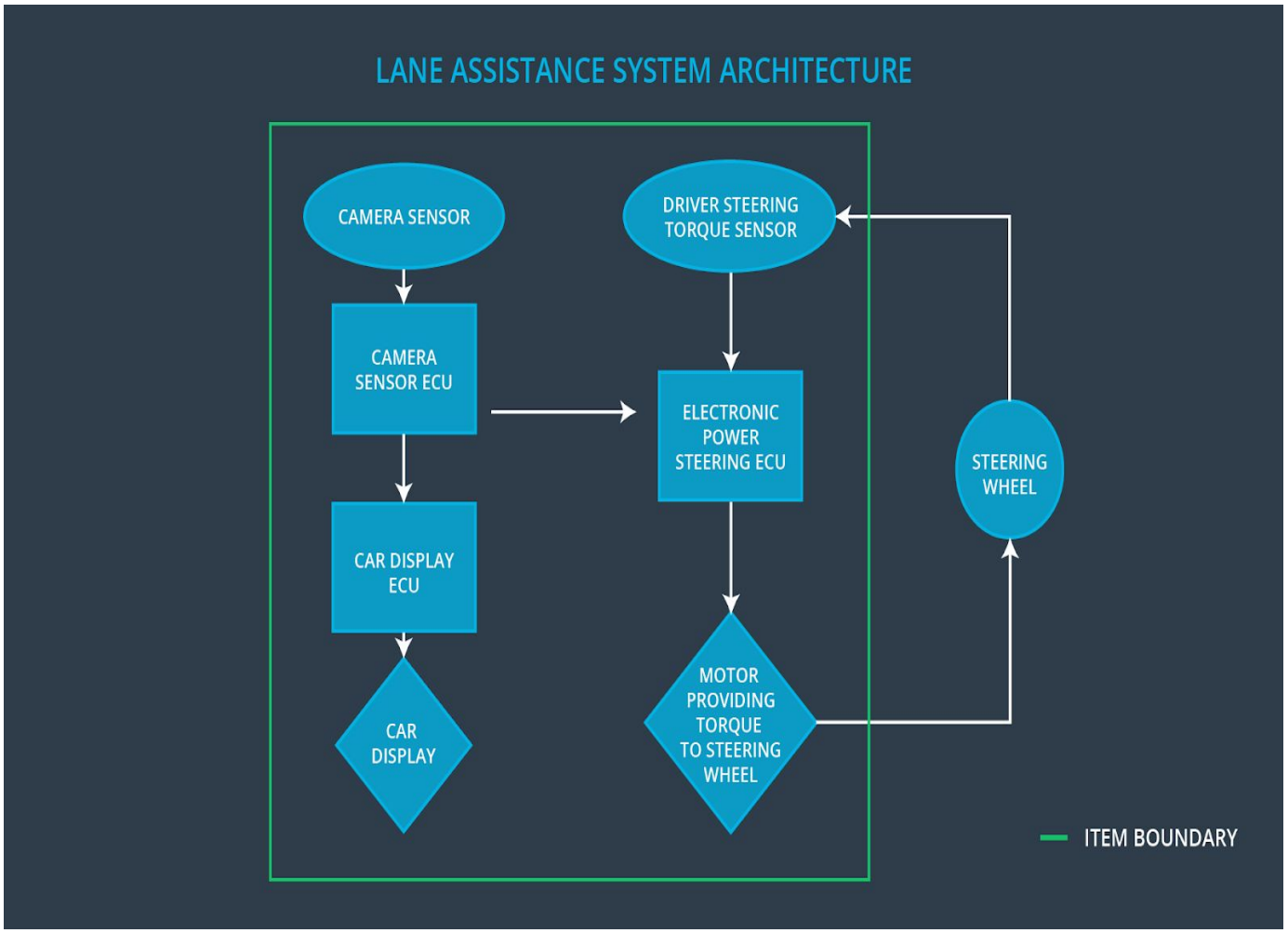
Purpose of functional safety concept is to determine which subsystems contains high level of risks and what is needed to prevent accidents. Here, we find out that which subsystems and elements can be used to meet safety goals. We also refine the safety goals further to come up with the functional safety requirements.

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 driver cannot misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	The camera system reads in images from the road.
Camera Sensor ECU	The camera sensor ECU detects when the vehicle has accidently departed it's lane and sends appropriate messages to car display ECU and the electronic power system ECU.

Car Display	Car display shows the information provided by the car display ECU.
Car Display ECU	Car display ECU receives the information from different subsystems including electronic power steering system and transfer it to car display
Driver Steering Torque Sensor	It measures the amplitude and frequency of the steering torque
Electronic Power Steering ECU	The power steering ECU determines the direction and the amount of power-assist according to the vehicle speed signals and signals from the steering torque sensor
Motor	The EPS motor is activated by the current from the power steering ECU and generates torque to assist the steering effort.

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

[Instructions: Fill in the functional safety analysis table below.]

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	MORE	The lane departure warning function applies an oscillating torque with very high

	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 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	50ms	Turn the system off after fault tolerant time interval
Functional Safety Requirement	The Lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Turn the system off after fault tolerant time interval

01-02				

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 value is reasonable. Test how drivers react to different Max_Torque_Amplitude values to find if the value is reasonable.	When the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. We do a software test by inserting a fault into the system and verify if the safety requirement is met
Functional Safety Requirement 01-02	Validate the Max_Torque_Frequency value is reasonable. Test how drivers react to different Max_Torque_Frequency values to find if the value is reasonable.	When the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. We do a software test by inserting a fault into the system and verify if the safety requirement is met

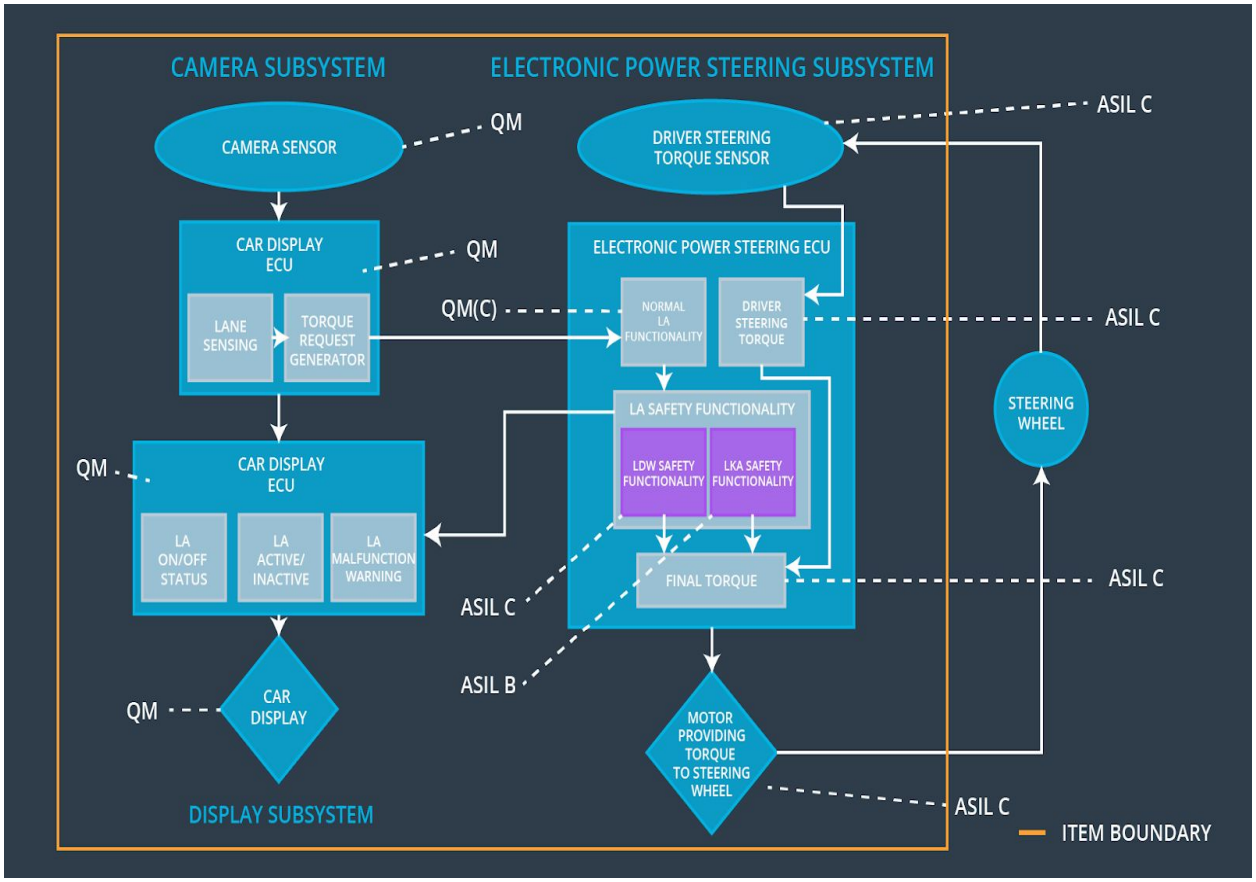
Lane Keeping Assistance (LKA) Requirements:

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 the system off after fault tolerant time interval

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 the Max_Duration value is reasonable. Test different Max_Duration values to find reasonable Max_Duration value to dissuade drivers from taking their hands off the wheel.	We verify that the system really does turn off if the lane keeping assistance 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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	□		

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

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the function	Malfunction_01 ,Malfunction_02	Yes	the driver will see a warning light on the dashboard when the system malfunctions.
WDC-02	Turn off the function	Malfunction_03	Yes	Manual would include a warning that the lane assistance system should not be used as an autonomous driving system and the driver maintains the

				responsibility of the safe operations of the vehicle