Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [1.0]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
27/11/2018	1	Archit Rastogi	First pass

Table of Contents

Purpose of the Functional Safety Concept

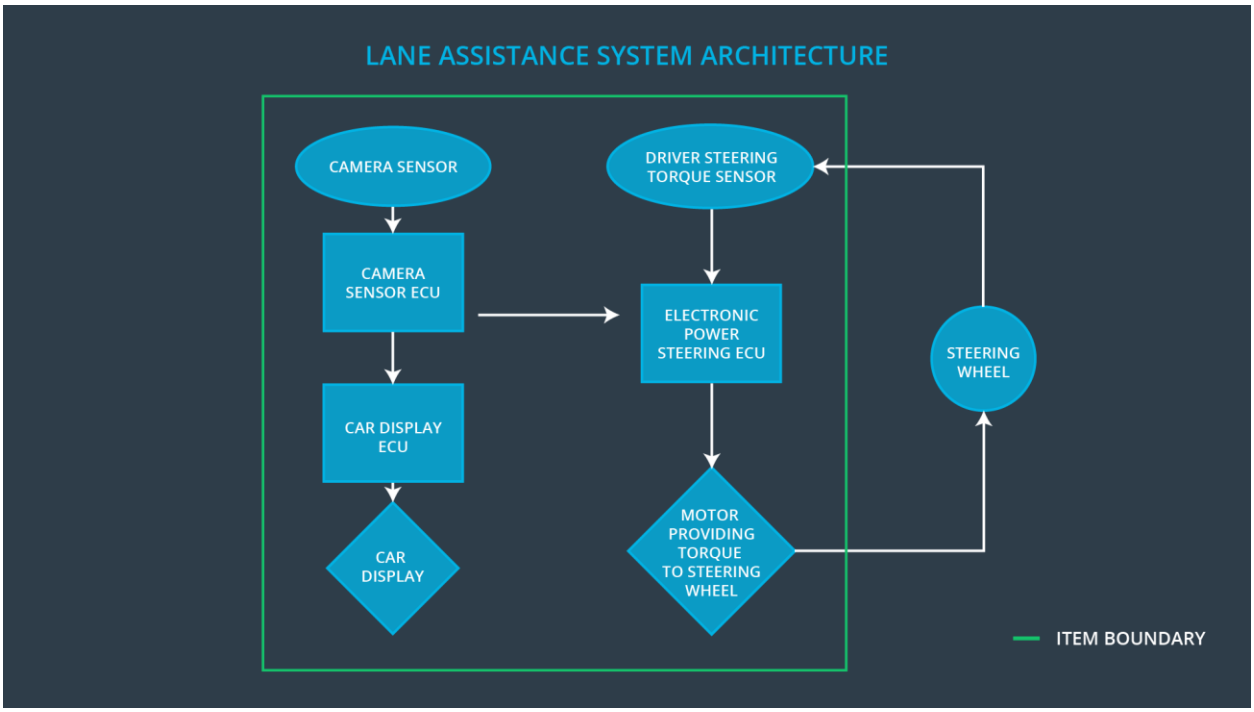
Functional Safety concept documents the high-level functional safety requirements identified from functional safety goals. These requirements are then allocated to the relevant parts of the system. Verification and validation for all the requirements is also documented. From the result of functional safety concept, technical requirements are derived at a later stage.

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

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Captures Image and provides the data to the Camera ECU
Camera Sensor ECU	Processes the images to calculate the car position with respect to lane lines
Car Display	Provides display warnings and status to the driver
Car Display ECU	Generates the warning signals based on input from Camera Sensor ECU and EPS ECU
Driver Steering Torque Sensor	Measures the steering torque applied by the driver
Electronic Power Steering ECU	Process the input from Driver Steering Torque sensor and Camera sensor ECU and provides the final torque based on the appropriate Lane Assistance functionality
Motor	Applies the final torque received from Electronic Power Steering ECU to 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 torque to provide the driver a haptic	MORE	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit)

	feedback		
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	Vibration Torque Amplitude below Max_Torque_Amplitude
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	Vibration Torque frequency 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	Validate Max_Torque_Amplitude chosen is appropriate for different drivers	Verify when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval
Functional Safety Requirement 01-02	Validate Max_Torque_Frequency chosen is appropriate for different drivers	when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval

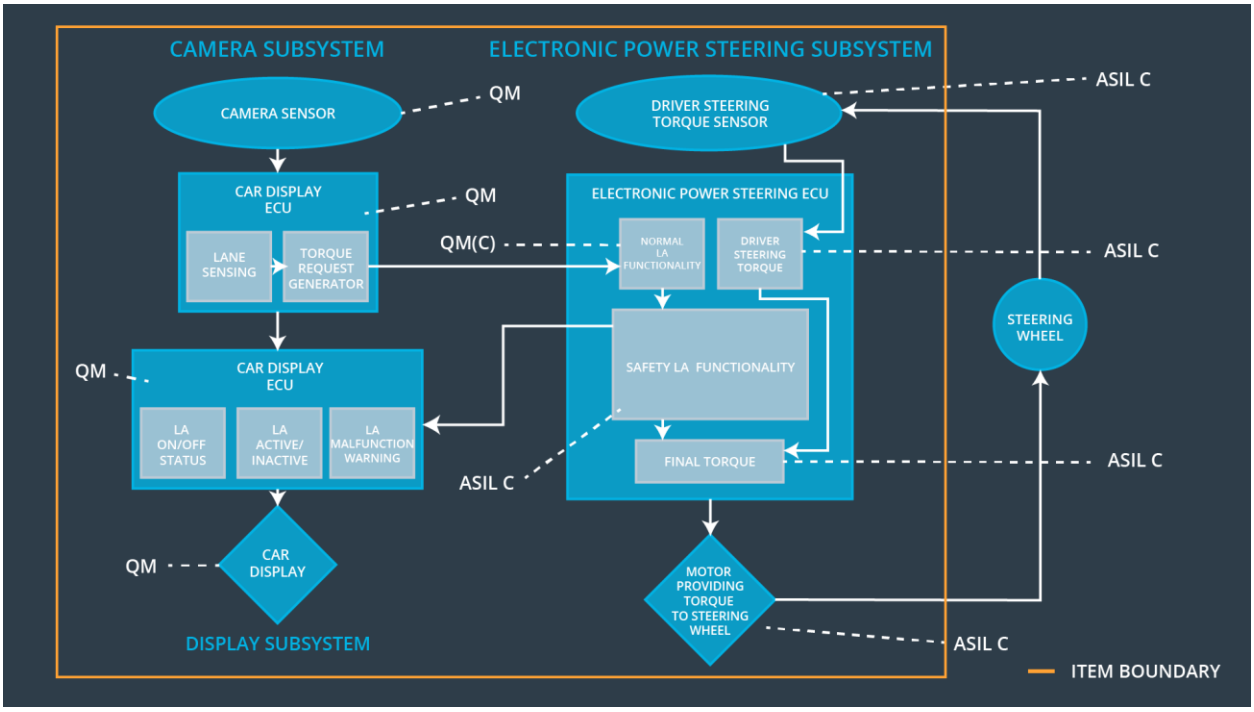
Lane Keeping Assistance (LKA) Requirements:

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	Lane Keeping Assistance Torque is zero

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 value chosen is appropriate for not allowing drivers to take their hands off the wheel	Verify that the functionality turns off if LKA exceeds 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	System off	Malfunction 01, 02	Yes	Warning on Car Display
WDC-02	System off	Malfunction 03	Yes	Warning on Car Display