Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
2019.06.28	1.0	Yuan.J	Initial Draft

Table of Contents

Table of Contents

Purpose of the Functional Safety Concept

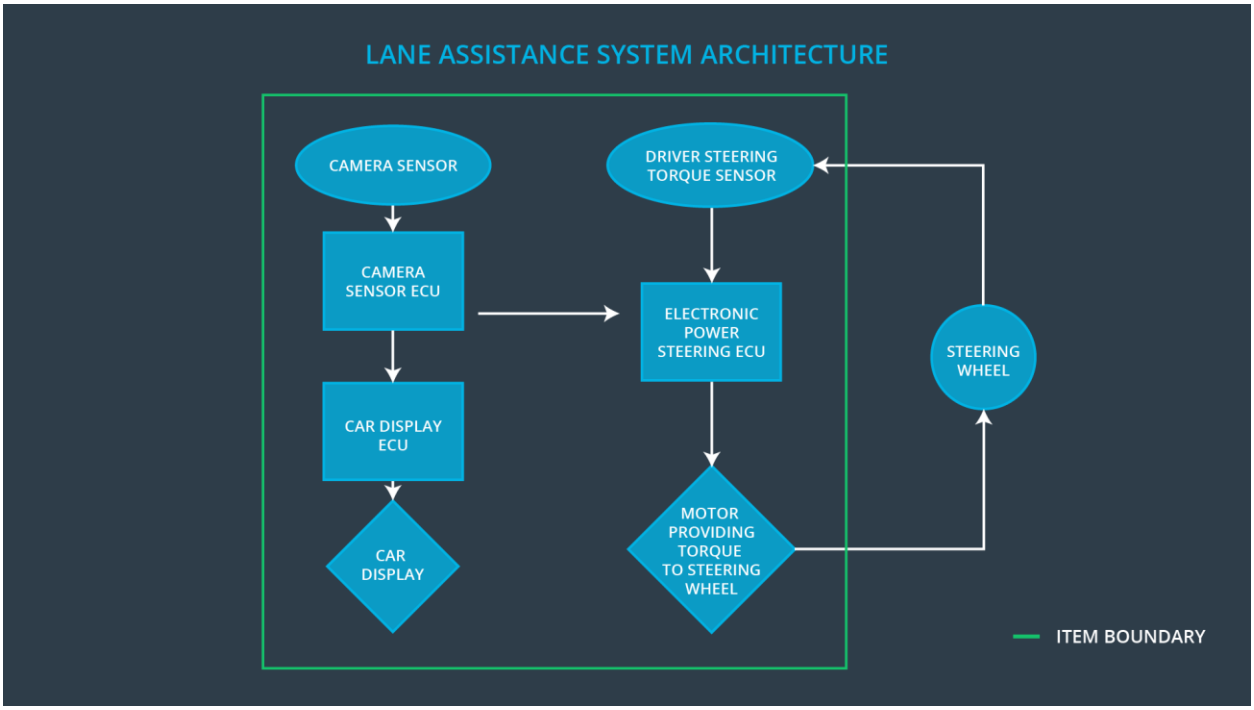
The purpose of the functional safety concept is to refine the high-level goals from Hazard Analysis and Risk Assessment and allocate these requirements to high level system diagrams for the lane assistance functional safety project as pertain to the different parts of the item architecture.

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 (LDW) function shall be limited
Safety_Goal_02	The lane keeping assistance (LKA) 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.
Safety_Goal_03	The camera sensor ECU shall check the LA on/off, active/inactive and malfunction warning status before sending torque requests to the lane departure warning system
Safety_Goal_04	The lane keeping assistance (LKA) function shall deactivate when the camera sensor stops detecting lanes and shall warn the driver of its deactivation.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Sensor responsible for capturing vehicle driving condition including detectable lane lines.
Camera Sensor ECU	Camera Sensor ECU responsible for identifying when the vehicle has accidentally departed its lane and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	Visual display responsible to displaying warning of LKA and LDW current state.
Car Display ECU	Car Display ECU responsible for displaying warning of LKA and LDW state on the Car Display.
Driver Steering Torque Sensor	Sensor responsible for measuring of steering torque which the driver is applying to the steering wheel.
Electronic Power Steering ECU	Electronic Power Steering ECU responsible for measuring the torque provided by the driver and output the torque request.
Motor	Generate and provide steering 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: DV04 - Actor effect	The lane departure warning function

	function shall apply an oscillating steering torque to provide the driver a haptic feedback	(torque amplitude) is too much	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: DV04 - Actor effect (torque frequency) is too much	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: DV03 - Function always activated (No limit)	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 Electronic Power Steering ECU shall ensure that the oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude	C	50ms	Set vibration torque amplitude to zero
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the oscillating torque frequence requested by the LDW function is below Max_Frequence_Amplitude	C	50ms	Set vibration torque amplitude to zero

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 if the MAX_Torque_Amplitude chosen is appropriate by testing with different drivers' reaction to different torque amplitudes.	Verify that the system really does turn off if the lane departure warning ever exceeded MAX_Torque_Amplitude
Functional Safety Requirement 01-02	Validate if the Max_Torque_Frequency chosen is appropriate by testing with different drivers' reaction to different torque amplitudes.	Verify that the system really does turn off if the lane departure warning ever exceeded MAX_Torque_Fequency

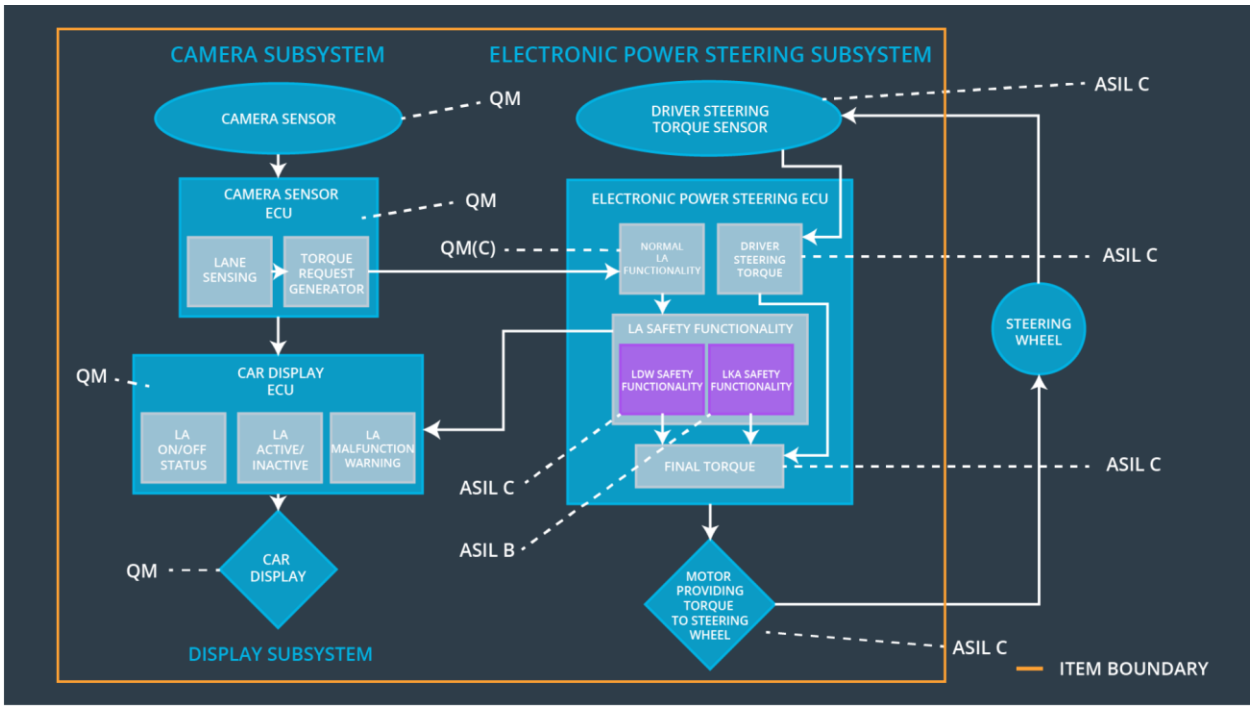
Lane Keeping Assistance (LKA) Requirements:

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	Set lane keeping Assistance torque to 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 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

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 LDW functionality	Torque amplitude is higher than Max_Torque_Amplitude	Yes, LDW torque shall be set to zero	LDW Inactive and Malfunction Warning will be display at the vehicle dashboard.
WDC-02	Turn off LDW functionality	Torque frequency is higher than Max_Torque_Frequency	Yes, LDW torque shall be set to zero	LDW Inactive and Malfunction Warning will be display at the vehicle dashboard.
WDC-03	Turn off LKA functionality	Duration of torque application is higher than ‘Max_Duration’	Yes, LKA torque shall be set to zero	LKA Inactive and Malfunction Warning will be display at the vehicle dashboard.