Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document History

Date	Version	Editor	Description
July 28, 2017	1.0	John Chen	Initial Draft
August 1, 2017	2.0	John Chen	Update after first review

Table of Contents

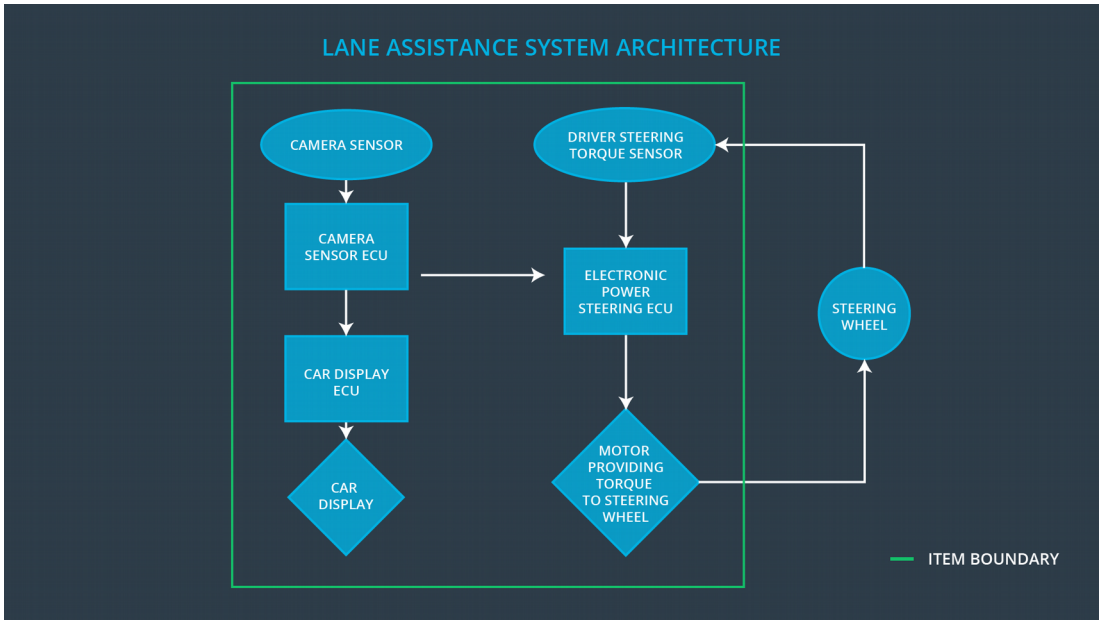
Purpose of the Functional Safety Concept

The purpose of the functional safety concept is to identify new system level requirements and allocate these requirements to high level system diagrams for the lane assistance functional safety project as pertain to the potential malfunctions of the electrical and electronic systems as defined by **ISO 26262** standard, tailored.

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 (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 road markings 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	Electronic Control Unit (ECU) responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
Car Display	Visual display responsible to displaying warning of lane departures and LKA and LDW activation and deactivations.
Car Display ECU	Electronic Control Unit (ECU) responsible for displaying warning of lane departures and LKA and LDW activation and deactivations on the Car Display.
Driver Steering Torque Sensor	Sensor responsible for measuring how much force (steering torque) the driver is applying to the steering wheel.
Electronic Power Steering ECU	Electronic Control Unit (ECU) responsible for measuring the torque provided by the driver and adding appropriate amount of torque based on a lane assistance system torque request (LKA), and vibrates the steering wheel when the driver drifts away from center by mistake (LDW).
Motor	Actuator responsible for applying requested torque to the steering column by the Electronic Power Steering ECU for either the LKA or the LDW functions.

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: DV04 - Actor effect (torque amplitude) is too much	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: 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.
Malfunction_04	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver with haptic feedback	WRONG: DV02 - Function unexpectedly activated	The lane departure warning function unexpectedly activates and starts oscillating the steering wheel during normal city driving.
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG: DV19 - Sensor detection is wrong	The lane keeping assistance function is not able to detect lane markings in darken tunnel.

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 amplitude to zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below MAX_Torque_Frequency	C	50 ms	Set vibration torque frequency 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 MAX_Torque_Amplitude chosen is high enough to be detected by driver while low enough not to cause loss of steering.	Verify that the system really does turn off if the lane departure warning ever exceeded MAX_Torque_Amplitude
Functional Safety Requirement 01-02	Validate MAX_Torque_Fequency chosen is high enough to be detected by driver while low enough not to cause loss of steering.	Verify that the system really does turn off if the lane departure warning ever exceeded MAX_Torque_Fequency

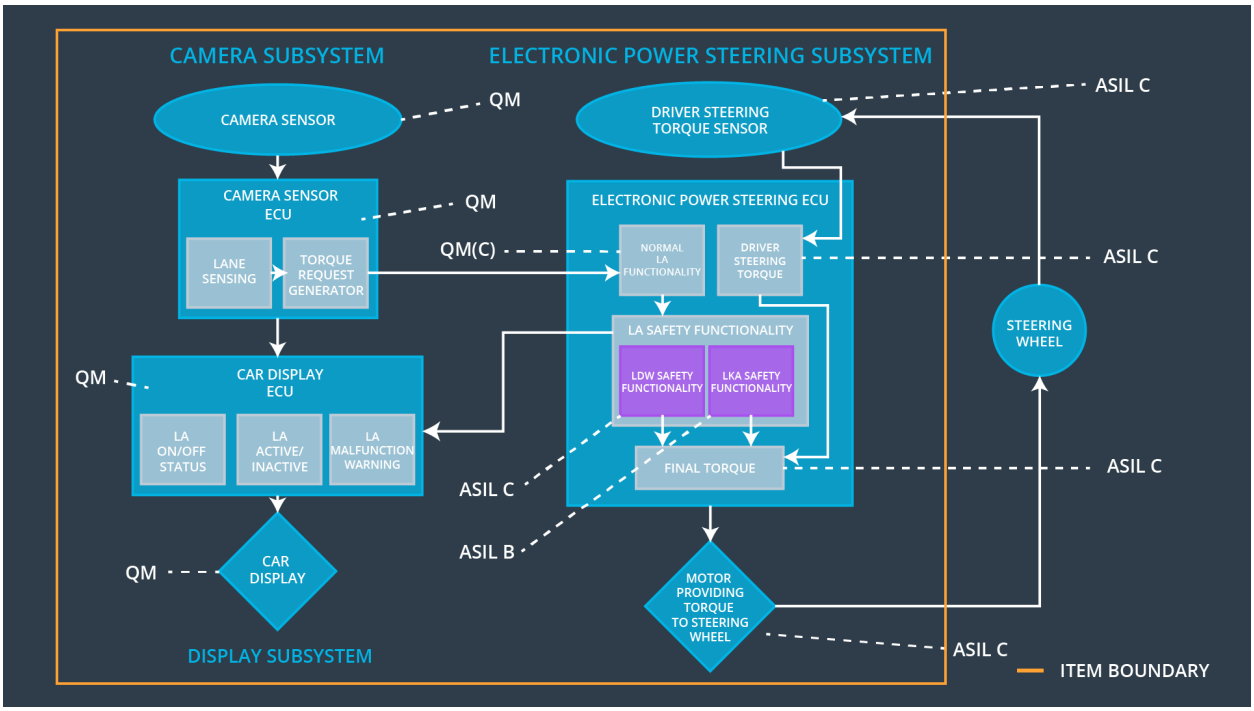
Lane Keeping Assistance (LKA) Requirements:

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	500 ms	Set lane keeping assistance torque to zero
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU stops detecting road markings and shall send its off status to the Car Display.	B	500 ms	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
Functional Safety Requirement 02-02	Validate Camera sensor ECU does not generate torque requests when lane sensing is lost.	Verify that the system really does turn off if the camera sensor ECU ever loses road marking detection.

Refinement of the System Architecture
Description of architecture elements



Element	Description
Camera Sensor	Sensor responsible for capturing vehicle driving condition including detectable lane lines.
Camera Sensor ECU - Lane Sensing	Software Module in the Camera Sensor ECU responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
Camera Sensor ECU - Torque request generator	Software Module in the Camera Sensor ECU responsible for calculating and sending the additional torque for the LDW and LKA functions.
Car Display	Visual display responsible to displaying warning of lane departures and LKA and LDW activation and deactivations.
Car Display ECU - Lane Assistance On/Off Status	Visual display responsible to displaying LKA and LDW ON/OFF status.
Car Display ECU - Lane Assistant	Visual display responsible to displaying displaying

Active/Inactive	warning of lane departures, LKA and LDW activation and deactivations.
Car Display ECU - Lane Assistance malfunction warning	Visual display responsible to displaying warning of LKA and LDW malfunctions.
Driver Steering Torque Sensor	Sensor responsible for measuring how much force (steering torque) the driver is applying to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software Module in the electronic power steering ECU responsible for receiving the Camera Sensor ECU torque requests.
EPS ECU - Normal Lane Assistance Functionality	Software Module in the electronic power steering ECU responsible for receiving the Driver Steering torque sensor input from the steering wheel.
EPS ECU - Lane Departure Warning Safety Functionality	Software Module in the electronic power steering ECU responsible for keeping the lane departure oscillating torque amplitude and frequence below MAX_Torque_Amplitude and MAX_Torque_Fequency respectively.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software Module in the electronic power steering ECU responsible for ensuring the application of the lane keeping assistance torque does not ever exceeded Max_Duration and if lane detection is lost, the LKA function is deactivated.
EPS ECU - Final Torque	Software Module in the electronic power steering ECU responsible for ensuring the LDW, LKA and the driver's steering torque requests are combined and sent to the Motor.
Motor	Actuator responsible for applying requested torque to the steering column by the Electronic Power Steering ECU for either the LKA or the LDW functions.

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**		
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU stops detecting road markings and shall send its off status to the Car Display.	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW functionality	Malfunction_01, Malfunction_02	Yes, LDW torque shall be set to zero	Lane Assist Inactive and Malfunction Warning will be set in the Car Display ECU
WDC-02	Turn off LKA functionality	Malfunction_03 Malfunction_05	Yes, LKA torque shall be set to zero	Lane Assist Inactive and Malfunction Warning will be set in the Car Display ECU