Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0
Released on 2017-10-29

Document history

Date	Version	Editor	Description
10/29/2017	1.0	Trevor Conley	First Submission

Table of Contents

Purpose of the Functional Safety Concept

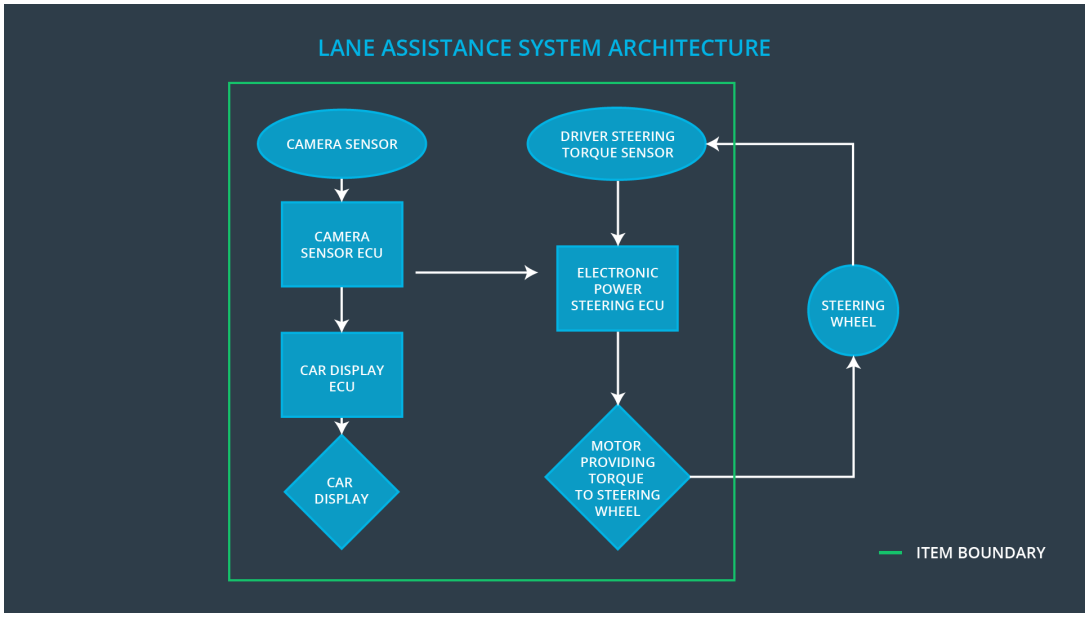
The purpose of the functional safety concept is to identify new system level requirements and allocate these requirements to high level system diagrams for the lane assistance functional safey project. These requirements will pertain to the potential malfunctions of the electrical and electronic systems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

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 and frequency for the lane departure warning function shall be limited.
Safety_Goal_02	The lane keeping assistance function shall have a time limit so that the driver may not misuse the function as a system for autonomous driving.
Safety_Goal_03	The camera sensor ECU shall check the Lane Assistance on/off, active/inactive and malfunction warning before sending a torque request to the lane departure warning system.
Safety_Goal_04	The lane keeping assistance function shall deactivate when the camera sensor stops detecting road markings and shall warn the driver that it has been deactivated.

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 has accidently departed its lane and sends the appropriate messages to the Car Display ECU and the Electronic Power ECU
Car Display	The Car Display is the visual indicator responsible for displaying the warning that the vehicle is departing the lane
Car Display ECU	The Car Display ECU is responsible for receiving signals from the Camera Sensor ECU if either the Lane Departure or Lane Keeping functions are activated
Driver Steering Torque Sensor	The Driver Steering Torque Sensor is responsbile for knowing how much torque is currently applied to the steering wheel
Electronic Power Steering ECU	The Electronic Power Steering ECU receives the torque request from the Camera Sensor ECU. It computes the residual torque amount to be applied and sends the torque output to the Motor
Motor	The Motor is responsible for applying the torque to the steering wheel in order to keep the car in the current lane

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	The lane departure warning function applies an oscillating torque higher than the 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 higher than the 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 assitance function is not limited in time which leads to a misuse as autonomous driving
Malfunction_04	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver with haptic feedback	WRONG	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	The lane keeping assistance function is not able to detect lane markings

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 0
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 virbration torque amplitude to 0

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 to not cause loss of steering	Verify that the system really does turn off if the lane departure warning ever exceeds MAX_TORQUE_AMPLITUDE
Functional Safety Requirement 01-02	Validate MAX_TORQUE_FREQUENCY chosen is high enough to be detected by driver while low enough to not cause loss of steering	Verify that the system really does turn off if the lane departure warning ever exceeds MAX_TORQUE_FREQUENCY

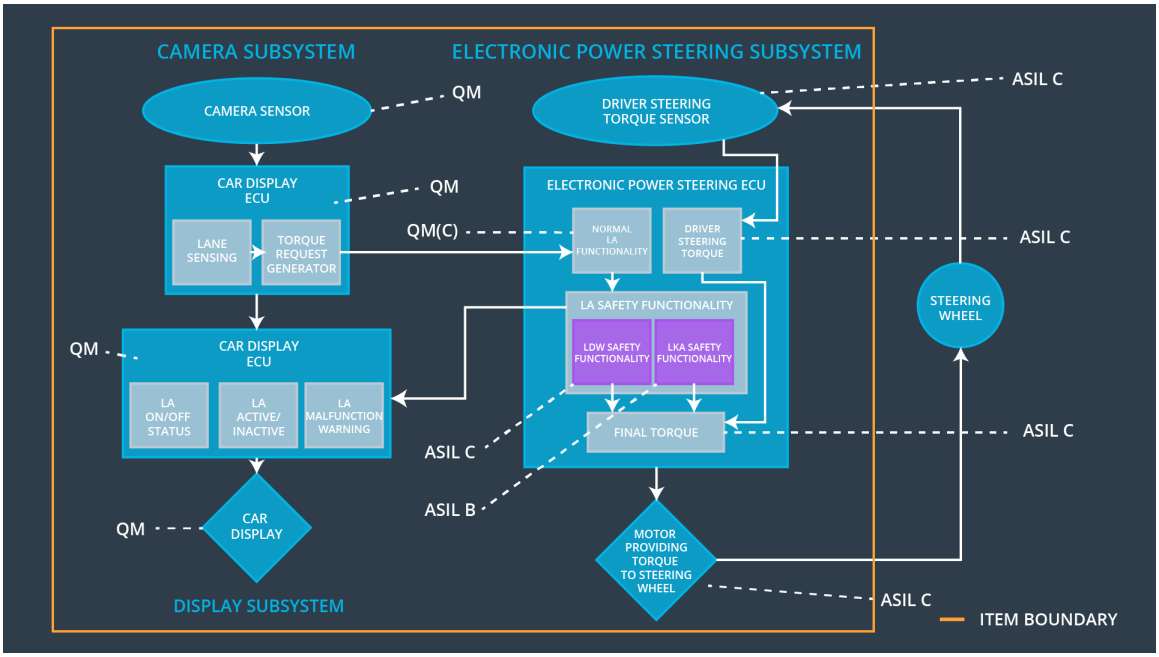
Lane Keeping Assistance (LKA) Requirements:

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 0
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to 0 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 0

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 prevent drivers from taking their hands off of the wheel	Verify that the system really does turn off if the lane keeping assistance every exceeds MAX_DURATION
Functional Safety Requirement 02-02	Validate Camera Sensor ECU does not generate torque requests when lane detecting goes away	Verfiy that the system really does turn off if lane markings are no longer detected

Refinement of the System Architecture



Element	Description
Camera Sensor	Sensor responsible for capturing vehicle diving condition including lane markings
Camera Sensor ECU - Lane Sensing	Software Module in the Camera Subsystem reponsible for detecting lane lines and determining when the vehicle mistakenly departs the lane
Camera Sensor ECU – Torque reqest generator	Software Module in the Camera Subsystem responsible for calculating and sending additional torque to the LDW and LKA functions
Car Display	Visual display responsible for displaying warning of lane departure and LDW and LKA activations/deactivations
Car Display ECU – Lane Assistance On/Off Status	Visual display responsible for displaying LDW and LKA status
Car Display ECU – Lane Assistance Active/Inactive	Visual display responsible for displaying the warning of lane departure, LDW and LKA activations/deactivations
Car Display ECU – Lane Assistance malfunction warning	Visual display responsible for displaying warning of LDW and LKA malfunctions

Driver Steering Torque Sensor	Sensor responsible for measuring how much 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 resquest
EPS ECU – Normal Assistance Functionality	Software Module in the Electronic Power Steering ECU responsible for receving 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 and frequency below the MAX_TORQUE_AMPLITUDE and MAX_TORQUE_FREQUENCY
EPS ECU – Lane Keeping Assistant Safety Functionality	Software Module in the Electronic Power Steering ECU responsible for ensuring the time of the lane departure oscillating torque freqeuncy and amplitude does not exceed MAX_DURATION, and if the lane 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 driver's steering torque requests are combined and sent to the motor
Motor	Provides torque to the steering wheel

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 amplitude 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 only applied for MAX_DURATION	**X**		
Functional Safety Requirement 02-02	The Electronic Power Steering ECU shall ensure that the lane keeping assistance torque is set to 0 when the Camera Sensor ECU stops detecting lane markings and shall send an ‘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 of LDW funcionality	Malfunction_01, Malfunction_02	Yes, LDW torque shall be 0	Lane Assistance inactive and Malfunction Warning will be set in the Car Display ECU
WDC-02	Turn off LKA functionality	Malfunction_03, Malfunction_04	Yes, LKA torque shall be 0	Lane Assistance inactive and Malfunction Warning will be set in the Car Display ECU