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
11/09/2017	1	JP	First Version

Table of Contents

Purpose of the Functional Safety Concept

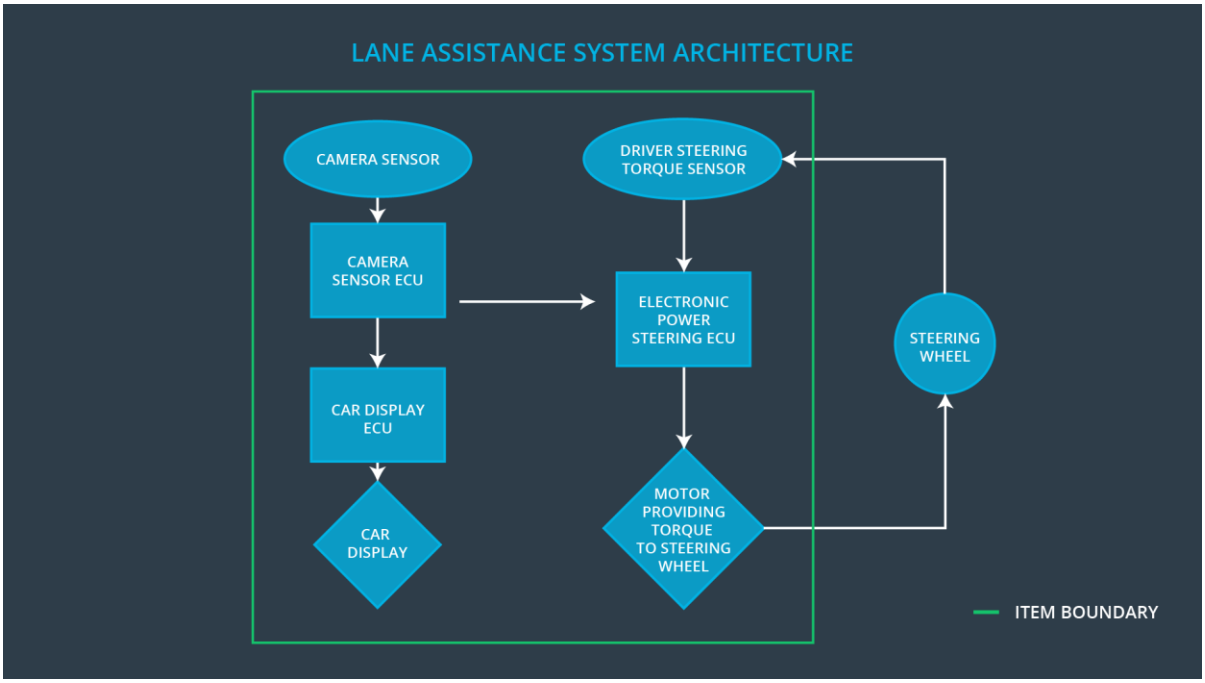
The purpose of the functional safety concept is to identify new system level requirements and allocate these requirements to high level system diagrams for the lane assistance functional safety project. These requirements will pertain to the potential malfunctions of the electrical and electronic systems 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	Is taking and sending an image stream to the camera sensor ECU
Camera Sensor ECU	Is detecting lane lines and determining when the vehicle leaves the lane by mistake.
Car Display	Is a visual display responsible for displaying warnings of lane departures and LKA activation and deactivation.
Car Display ECU	Is responsible for displaying warning of lane departures and LKA and LDW activation and deactivation on the Car display.
Driver Steering Torque Sensor	Is responsible for measuring the torque provided by the driver.
Electronic Power Steering ECU	Is receiving 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	Is executing the torque request of the electronic power steering ECU and provides 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) 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 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.

Malfunction_04	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 amplitude (above limit)
Malfunction_05	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 deactivated during heavy steering input by the driver.

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 LDW 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 LDW shall ensure that the lane departure oscillating torque frequency is below MAX_Torque_Frequency	C	50 ms	Set vibration torque frequency 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 not to cause loss of steering	Verify that the system really does turn off it the lane departure warning ever exceeded MAX_Torque_Amplitude

Functional Safety Requirement 01-02	Validate MAX_Torque_Frequency 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_Frequency.

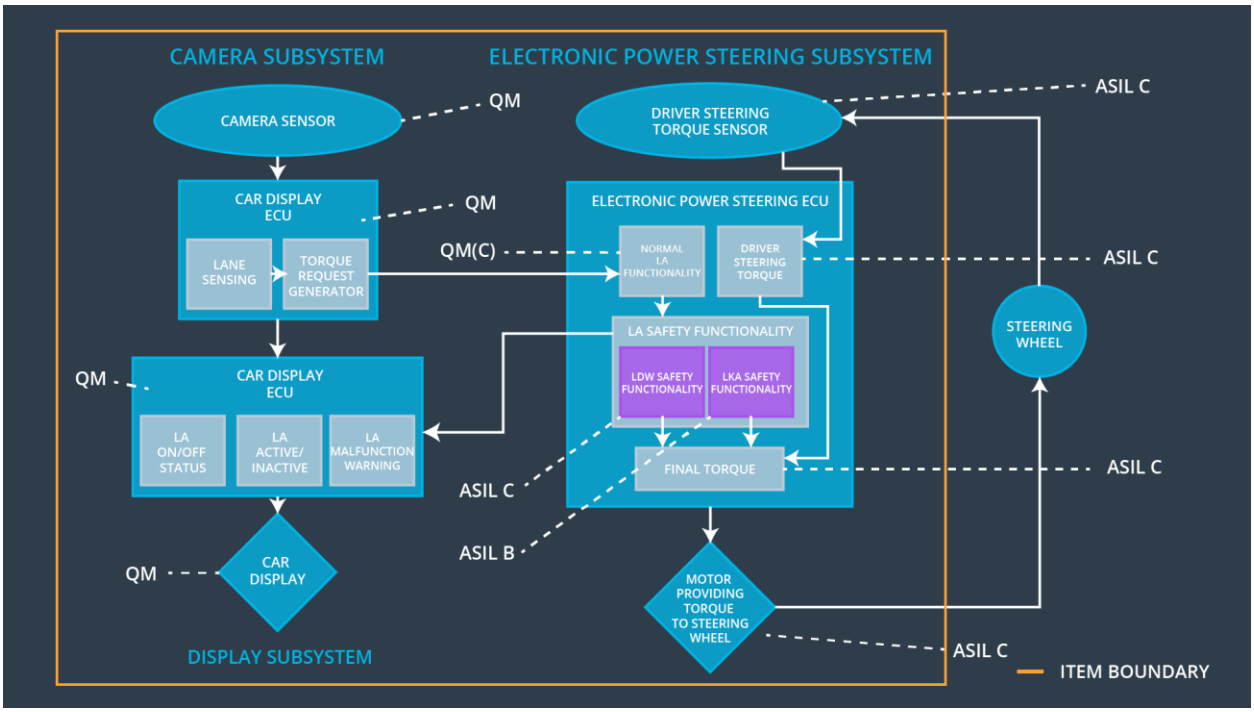
Lane Keeping Assistance (LKA) Requirements:

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	500ms	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 zero when the camera sensor ECU stops detecting road markings and shall send its off status to Car Display	B	500ms	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 dis 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 request 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



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 LDW shall ensure that the lane departure oscillating torque amplitude is below MAX_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The LDW shall ensure that the lane departure oscillating torque frequency is below MAX_Torque_Frequency	**X**		
Functional Safety Requirement	The electronic power steering ECU shall ensure that the lane keeping assistance torque is	**X**		

02-01	applied for only Max_Duration.			
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 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, Malfunction_04	Yes	LED on car display
WDC-02	Turn off LKA functionality	Malfunction_03, Malfunction_05	Yes	LED on car display