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
21/6/2018	1.0	Sameer Negi	Initial Version of Functional Safety Concept

Table of Contents

Purpose of the Functional Safety Concept

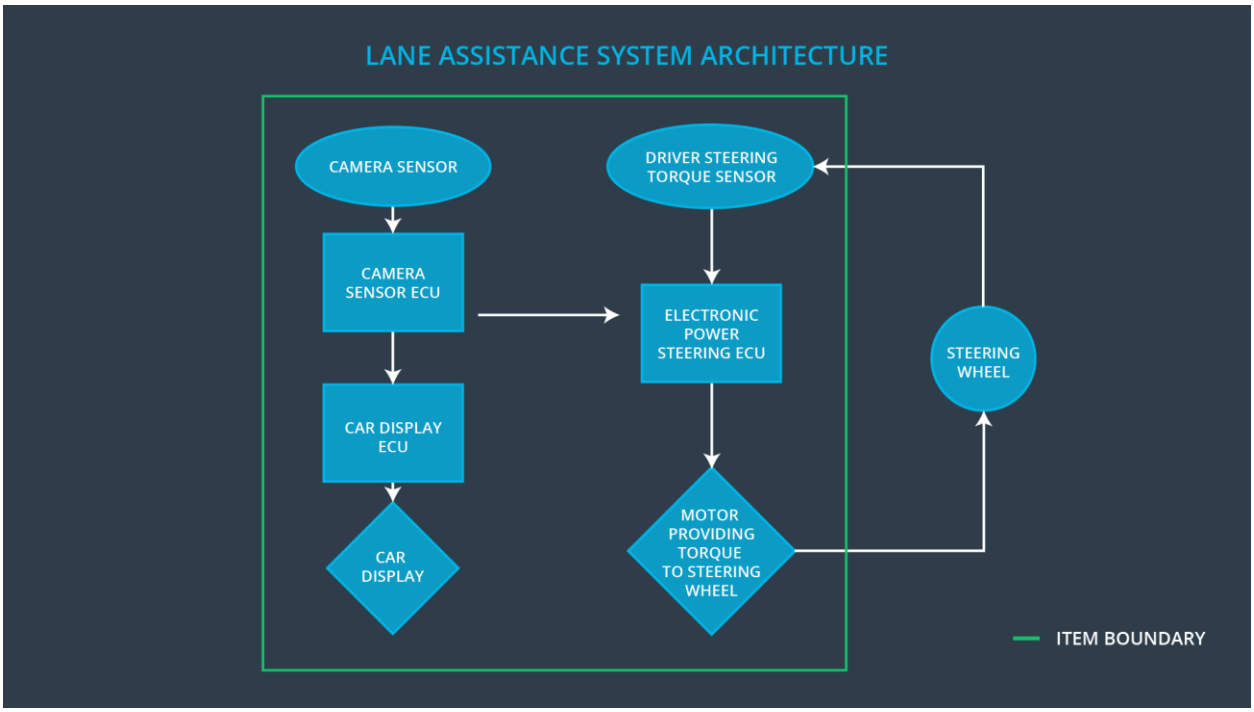
The purpose of the functional safety concept is to describe the implementation of the independent safety solutions for a defined item.

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 lane detection shall not be activated if the detection for a certain environment is not reliable.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	A sensor for acquiring environment information as image.
Camera Sensor ECU	Electronic Control Unit (ECU) responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.

Car Display	Provide feedback to the driver displaying warnings and the Lane Departure Assistance status
Car Display ECU	Receives signals from the camera ECU if either of the functions have been activated
Driver Steering Torque Sensor	A sensor that acquires the torque value of the steering wheel
Electronic Power Steering ECU	Receives the vibrational torque request from the camera ECU. Computes the residual torque needed to be applied after taking into account the input from the torque sensor. Sends the torque output request 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.

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	MORE	The lane keeping assistance function is

	an oscillating steering torque to provide the driver a haptic feedback		not limited in time duration which leads to misuse as an autonomous driving function.
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 lead to misuse as an lane 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 lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Lane Departure warning function is not activated
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50ms	Vibration frequency is 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	Set oscillating torque amplitude to Max_Torque_Amplitude causes the light warning to be turned on	when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant

01-01		
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

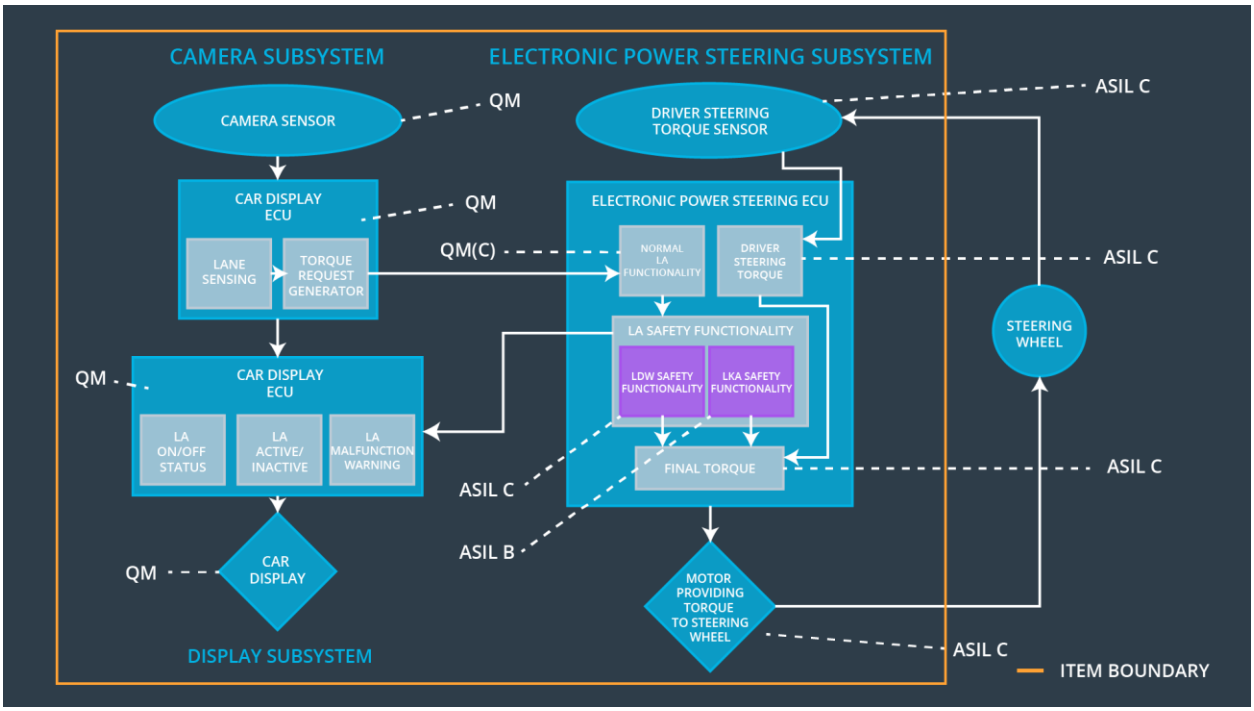
Lane Keeping Assistance (LKA) Requirements:

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 only Max_Duration.	B	500 ms	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 chosen really did dissuade drivers from taking their hands off the wheel.	The system really does turn off if the lane keeping assistance every 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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**Yes**	**No**	**No**
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	**Yes**	**No**	**No**
Functional	The electronic power steering	**Yes**	**No**	**No**

Safety Requirement 02-01	ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off functionality	The malfunction of the steering wheel vibrating too much	Yes	Warning light on the dashboard
WDC-02	Turn off functionality	The malfunction of the lane keeping assistance function being applied for too long	Yes	Warning light on the dashboard