Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0
08-25-2017

Document History

Date	Version	Editor	Description
08-25-2017	1.0	Neil Hiddink	Functional Safety Concept for Lane Assistance Functionality.

Table of Contents

Purpose of the Functional Safety Concept

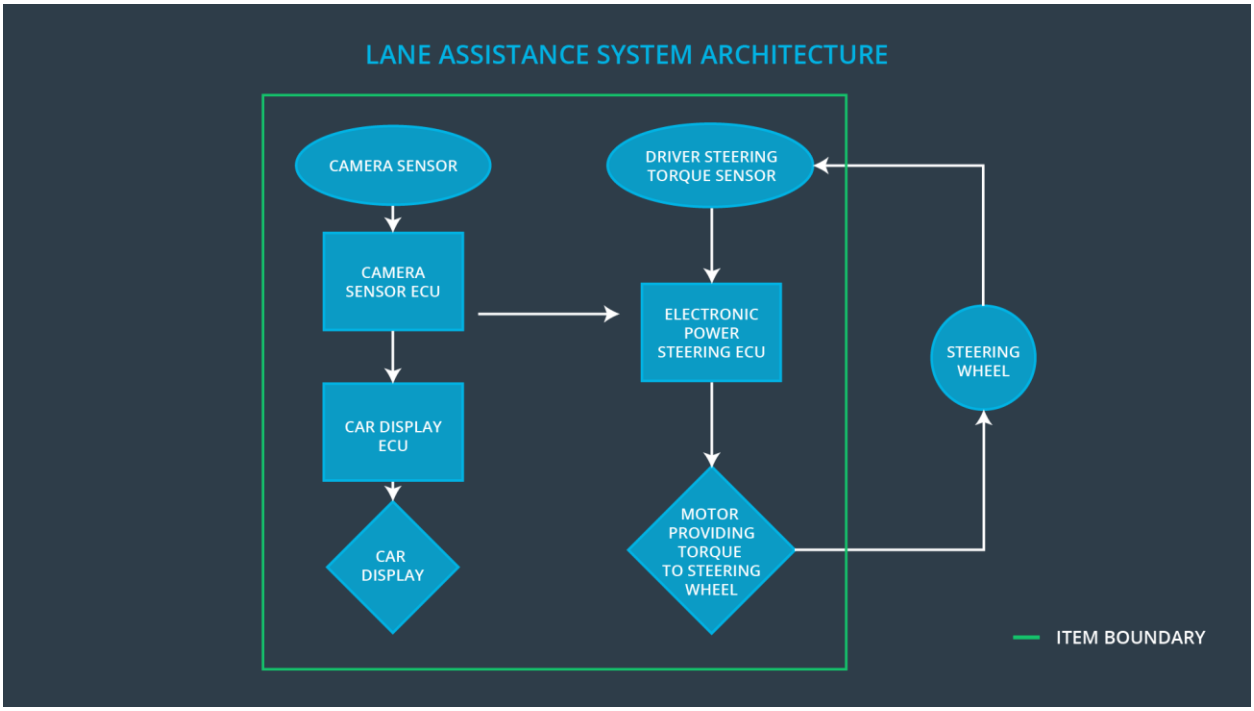
The purpose of this functional safety concept is to avoid accidents by reducing risks involved in the Lane Assistance functionality to acceptable levels. Additionally, the functional safety concept relates the Lane Assistance item to high-level architecture diagrams in order to facilitate discussions around its general functionality.

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 function shall be limited.
Safety_Goal_02	The Lane Assistance functionality 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.

Preliminary Architecture



Description of Architecture Elements

Element	Description
Camera Sensor	A sensor (or array of sensors) mounted on the front of the vehicle that collects image and video data.
Camera Sensor ECU	A computer that simultaneously handles steering corrections for the power steering ECU and warning messages for the car display ECU by interpreting the data collected by the camera sensor.
Car Display	A physical display component mounted inside the vehicle that provides visual feedback to the driver.
Car Display ECU	A computer within the car display component that is responsible for relaying warning messages to the driver as received from the camera sensor ECU.
Driver Steering Torque Sensor	A sensor that measures the torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	A computer within the power steering column that is responsible for controlling the torque applied to the steering wheel according to the action relayed from the camera sensor ECU or in response to an under- and/or over-compensation of torque by the driver.
Motor	The component responsible for applying the work required to produce the torque required to execute actions delivered to the power steering ECU.

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.

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 Assistance item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Turn Off System
Functional Safety Requirement 01-02	The Lane Assistance item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Turn Off System

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	Prove that the value chosen for Max_Torque_Amplitude is appropriate by testing how drivers react to different torque amplitudes.	When the torque amplitude exceeds Max_Torque_Amplitude, the output of the Lane Assistance item is set to zero within a fault tolerant time interval of 50 milliseconds.
Functional Safety Requirement 01-02	Prove that the value chosen for Max_Torque_Frequency is appropriate by testing how drivers react to different torque frequencies.	When the torque frequency exceeds Max_Torque_Frequency, the output of the Lane Assistance item is set to zero within a fault tolerant time interval of 50 milliseconds.

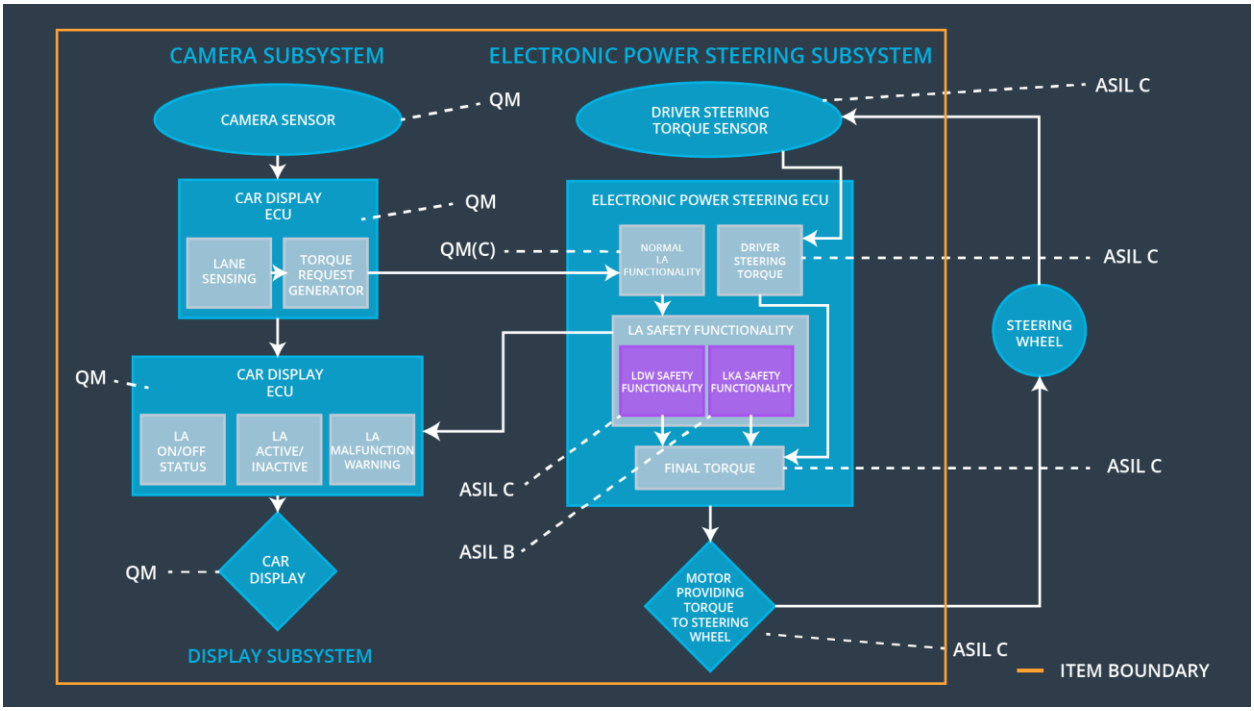
Lane Keeping Assistance (LKA) Requirements:

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	Turn Off System

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	Test that the value chosen for Max_Duration dissuades drivers from taking their hands off the wheel.	The system does turn off when the lane keeping assistance exceeds 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 Assistance item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	✓		
Functional Safety Requirement 01-02	The Lane Assistance item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	✓		
Functional Safety Requirement 02-01	The electronic power steering 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 the functionality.	Malfunction_01 Malfunction_02	Yes	Car Display
WDC-02	Turn off the functionality.	Malfunction_03	Yes	Car Display