Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12-25-2018	1.0	Eduardo Paz	Initial release

Table of Contents

Purpose of the Functional Safety Concept

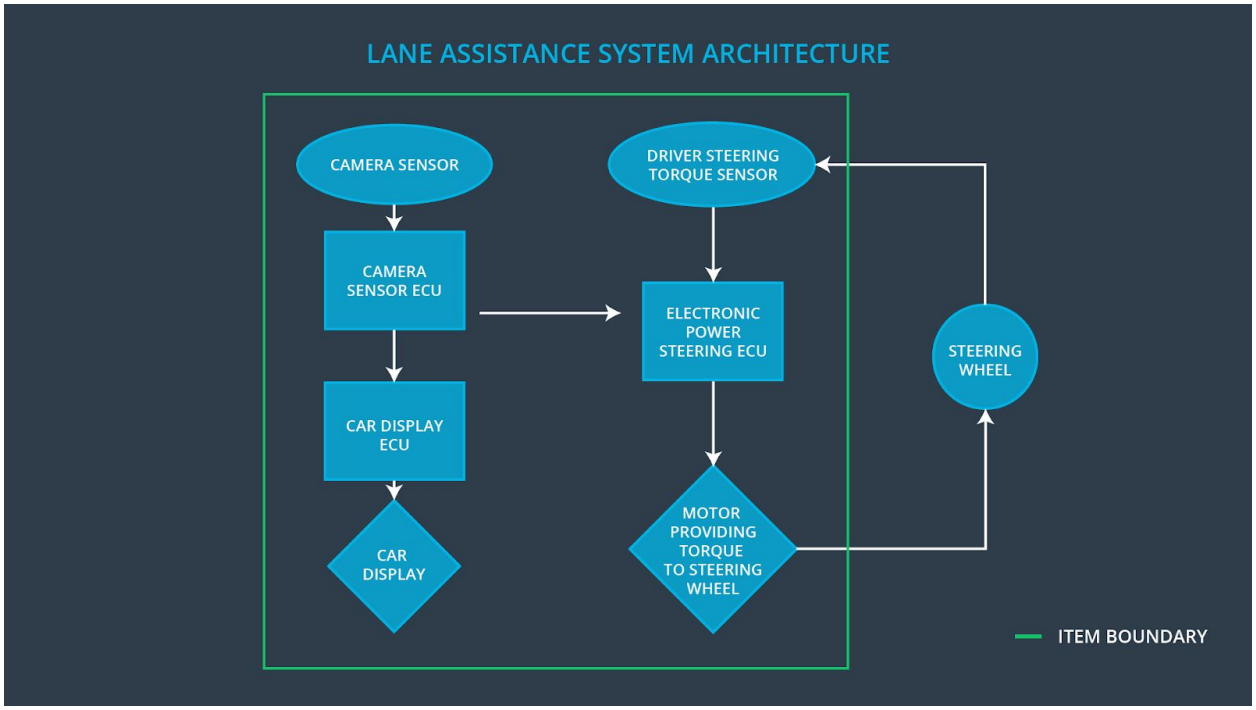
The Functional Safety Concept document will look at the system from a higher level identifying which subsystems and elements can be used to meet safety goals, and deriving the functional safety requirements.

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 additional steering torque from the lane keeping assistance function shall be limited, and 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	Reads in images from the road
Camera Sensor ECU	Identifies when the vehicle has accidentally departed its lane, and sends appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	Display useful information to the driver
Car Display ECU	Controls the display of information to the user
Driver Steering Torque Sensor	Monitors how much torque is applied to the steering wheel
Electronic Power Steering ECU	Controls how much torque will be applied to the steering wheel motor
Motor	Applies the 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 LDW 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 LDW 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 LKA function 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	LDW oscillating amplitude is set 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	LDW oscillating frequency is set 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	Max_Torque_Amplitude is set to 5cm.	LDW oscillating amplitude is set to 0 when above Max_Torque_Amplitude
Functional Safety Requirement 01-02	Max_Torque_Frequency is set to 100mS	LDW oscillating frequency is set to 0 when above Max_Torque_Frequency

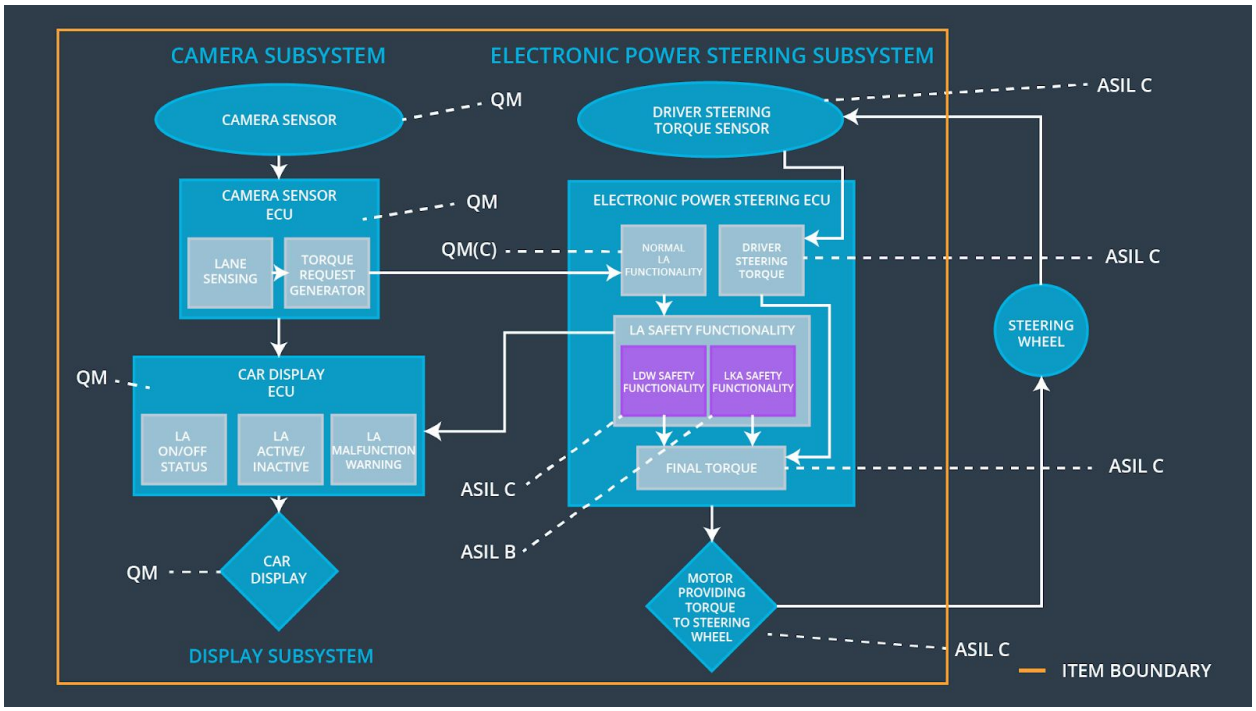
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving	B	500 ms	The LKA is turned off

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	The duration for LKA is set to 500mS	The LKA is turned off after 500 ms

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 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 lane keeping item shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Deactivate the LDW feature	Torque amplitude above Max_Torque_Amplitude, or Torque frequency above Max_Torque_Frequency	Yes	LDW feature deactivated on the Car Display
WDC-02	Deactivate the LKA feature	LKA feature activated for more than Max_Duration	Yes	LKA feature deactivated on the Car Display