Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
10/04/2017	1.0	Ibis Prevedello	First draft
10/18/2017	1.1	Ibis Prevedello	Correct FTTI for Functional Safety Requirement 02-01

Table of Contents

Document history 2
Table of Contents 3
Purpose of the Functional Safety Concept 4
Inputs to the Functional Safety Concept 5
  Safety goals from the Hazard Analysis and Risk Assessment 5
  Preliminary Architecture 5
    Description of architecture elements 6
Functional Safety Concept 7
  Functional Safety Analysis 7
  Functional Safety Requirements 7
  Refinement of the System Architecture 9
  Allocation of Functional Safety Requirements to Architecture Elements 9
  Warning and Degradation Concept 10

Purpose of the Functional Safety Concept

The purpose of the functional safety concept is to avoid accidents by reducing risks to acceptable levels.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	Oscillating steering torque should be limited for the Lane Departure Warning.
Safety_Goal_02	Steering torque should be time limited for the Lane Keep Assistance.
Safety_Goal_03	Steering torque should be disabled when the vehicle is driving backwards.

Preliminary Architecture

Figure 1 shows an overall Lane Assistance System Architecture, presenting how the systems are connected between them and the Steering Wheel.

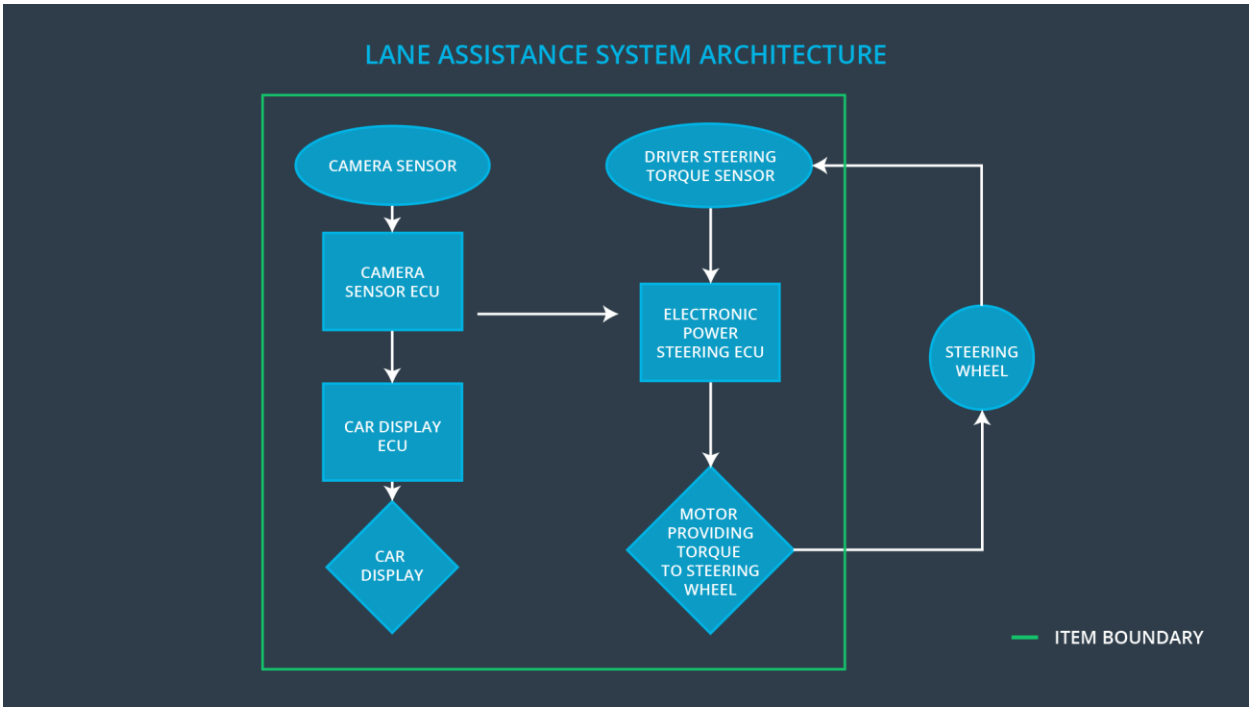

Figure 1 - Lane Assistance System Architecture

Description of architecture elements

Element	Description
Camera Sensor	A sensor positioned in the front of the car which will capture images and sends to the Camera Sensor ECU.
Camera Sensor ECU	The Electronic Central Unit responsible to process the image from the Camera Sensor and convert this image into useful data for the other systems.
Car Display	Display that takes data from the Car Display ECU and shows to the driver in form of lighted icons and audio warnings.
Car Display ECU	Electronic Central Unit that collects data from other systems and decide which kind of signal the Car Display needs to show.
Driver Steering Torque Sensor	Sensor that measures the steering torque that the driver is applying on the steering wheel.
Electronic Power Steering ECU	Electronic Central Unit that process the data collected by the Driver Steering Torque Sensor.
Motor	Receives the command from the Electronic Power Steering ECU and converts to torque on 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency
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 item shall ensure that the lane keeping assistance torque is applied for only Max_Duration

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 oscillating torque amplitude is below	C	50 ms	LDW is turned off with a lighted icon on the car display and/or

	Max_Torque_Amplitude.			sound warning to the driver.
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Amplitude.	C	50 ms	LDW is turned off with a lighted icon on the car display and/or sound warning to the driver.

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	Test the LDW with torque amplitude above Max_Torque_Amplitude and assure that the LDW function is turned off and indicated by a lighted icon and/or sound to the driver.	Verify the LDW function with values less than Max_Torque_Amplitude. Verify the LDW function turn off and the driver is alerted by a lighted icon and/or sound.
Functional Safety Requirement 01-02	Test the LDW with torque amplitude above Max_Torque_Frequency and assure that the LDW function is turned off and indicated by a lighted icon and/or sound to the driver.	Verify the LDW function with values less than Max_Torque_Frequency. Verify the LDW function turn off and the driver is alerted by a lighted icon and/or sound.

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 assistance torque is applied for a maximum of Max_Duration.	B	500 ms	LKA is turned off with a lighted icon on the car display and/or sound warning to the driver.

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 the LKA for a time above Max_Duration and assure that the LKA function is turned off and indicated by a lighted icon and/or sound to the driver.	Verify the LKA function with duration less than Max_Duration. Verify the LKA function turn off and the driver is alerted by a lighted icon and/or sound.

Refinement of the System Architecture

Figure 2 presents a refined system architecture including all the ASIL labels of each subsystem of the systems used.

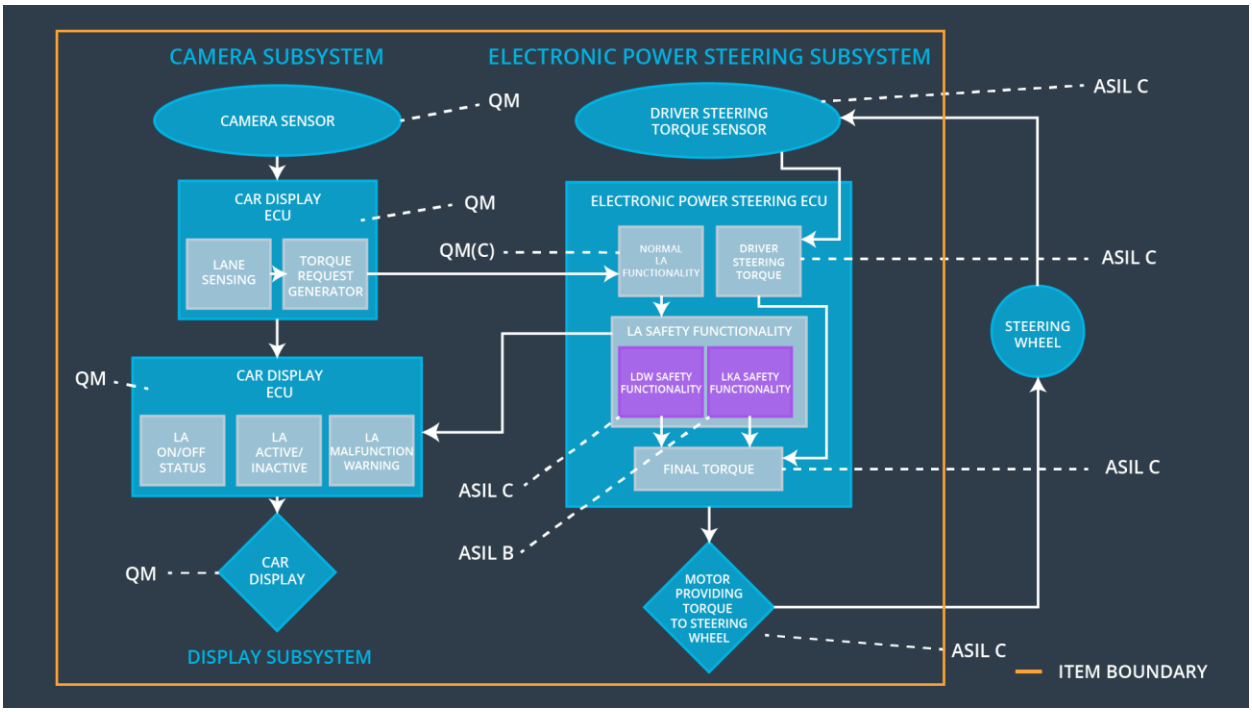

Figure 2 - Refined System Architecture

Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety	The Electronic Power Steering	X		

Requirement 01-01	ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.			
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the lane assistance torque is applied for a maximum of Max_Duration.	**X**		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	LDW is turned off with a lighted icon on the car display and/or sound warning to the driver.	LDW torque exceeds Max_Torque_Amplitude or Max_Torque_Frequency	YES	Lighted icon on the car display and/or sound warning to the driver.
WDC-02	LKA is turned off with a lighted icon on the car display and/or sound warning to the driver.	LKA torque is applied for a time longer than Max_Duration	YES	Lighted icon on the car display and/or sound warning to the driver.