Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
10.09.2017	1.0	Sergei Dmitriev	Initial version

Abbreviation List

N	Abbreviation	Definition
1.	ASIL	Automotive Safety Integrity Level
2.	ECU	Electronic Control Unit
3.	LDW	Lane Departure Warning
4.	LKA	Lane Keeping Assistance

Table of Contents

Document history 2
Abbreviation List 2
Table of Contents 2
Purpose of the Functional Safety Concept 3
Inputs to the Functional Safety Concept 3
Safety goals from the Hazard Analysis and Risk Assessment 3
Preliminary Architecture 3
Description of architecture elements 4
Functional Safety Concept 5
Functional Safety Analysis 5
Functional Safety Requirements 5
Refinement of the System Architecture 7
Allocation of Functional Safety Requirements to Architecture Elements 8
Warning and Degradation Concept 8

Purpose of the Functional Safety Concept

The purpose of the Functional Safety Concept is to refine the functional safety goals into functional safety requirements and allocate them to appropriate place in the item architecture.

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 LDW function shall be limited
Safety_Goal_02	The LKA function shall be time limited and the additional steering torque shall end after a given time interval

Preliminary Architecture

The Lane Assistance System architecture is shown in **Figure 1**.

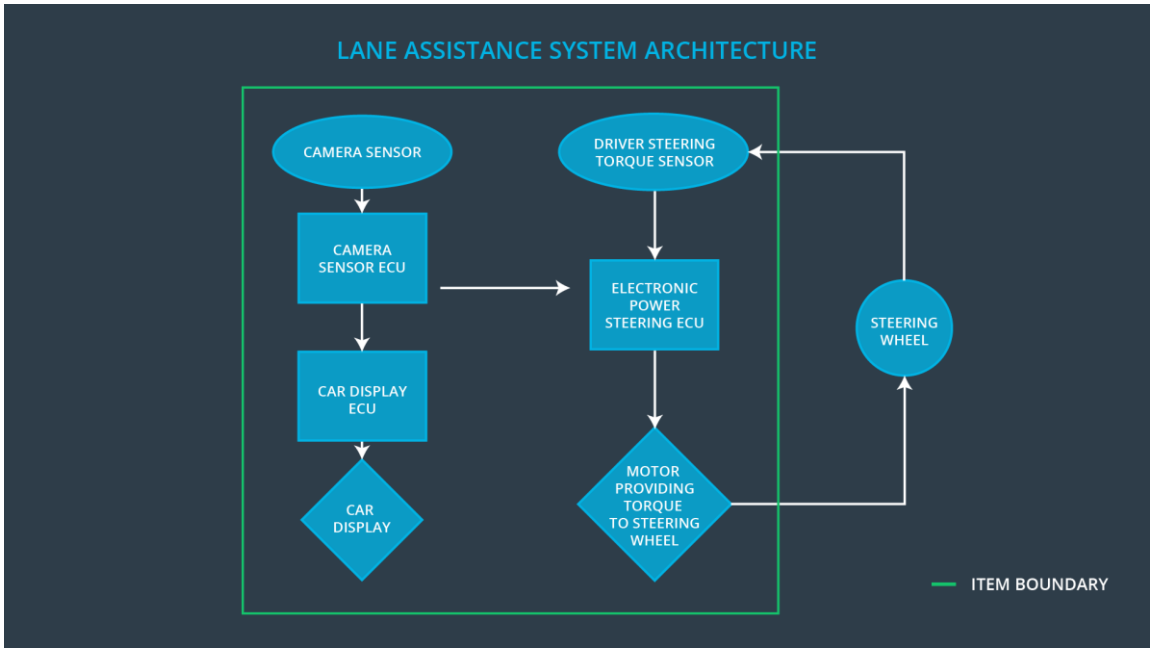

Figure 1

Description of architecture elements

Element	Description
Camera Sensor	The Camera Sensor reads in images from the road
Camera Sensor ECU	The Camera Sensor ECU identifies when the vehicle has accidentally departed its lane, and sends signals to Car Display and torque request to Electronic Power Steering ECU
Car Display	The Car Display shows a driver warn signals from Camera Sensor ECU processed by the Car Display ECU
Car Display ECU	The Car Display ECU processes signals from the Camera Sensor ECU and sends a signal to the Car Display to turn on/off appropriate status alarm
Driver Steering Torque Sensor	The Driver Steering Torque Sensor measures steering torque provided by the driver
Electronic Power Steering ECU	The Electronic Power Steering ECU defines the final torque for the Motor
Motor	The Motor provide torque to 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	The 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	The 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	The LKA function shall apply the steering torque when active in order to stay in ego lane	NO	The LKA 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	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below MAX_Torque_Amplitude	C	50 ms	The LDW torque request shall be set to zero

01-01				
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	The LDW torque request shall be set to zero

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	Method: Testing how drivers react to different vibrational torque amplitudes set for MAX_Torque_Amplitude Acceptance Criteria: All drivers had not difficulty controlling the vehicle because the steering wheel vibration	Method: Software testing. Set vibrational torque amplitudes more than MAX_Torque_Amplitude Acceptance Criteria: The lane assistance system torque output is set to zero within the 50 ms fault tolerant time interval
Functional Safety Requirement 01-02	Method: Testing how drivers react to different torque frequency set for MAX_Torque_Frequency Acceptance Criteria: All drivers had not difficulty controlling the vehicle because the steering wheel vibration	Method: Software testing. Set vibrational torque frequency more than MAX_Torque_Frequency Acceptance Criteria: The lane assistance system torque output is set to zero within the 50 ms fault tolerant time interval

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 ensure that the LKA torque is applied for only Max_Duration	B	500 ms	The LKA torque request shall be set to 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	Method: Testing how drivers react to different duration of the LKA torque request set for Max_Duration Acceptance Criteria: No drivers were dissuaded from taking their hands off the wheel	Method: Software testing. Set duration of the LKA torque request more than Max_Duration Acceptance Criteria: The lane assistance system torque output is set to zero within the 500 ms fault tolerant time interval

Refinement of the System Architecture

Refined system architecture is shown in **Figure 2**.

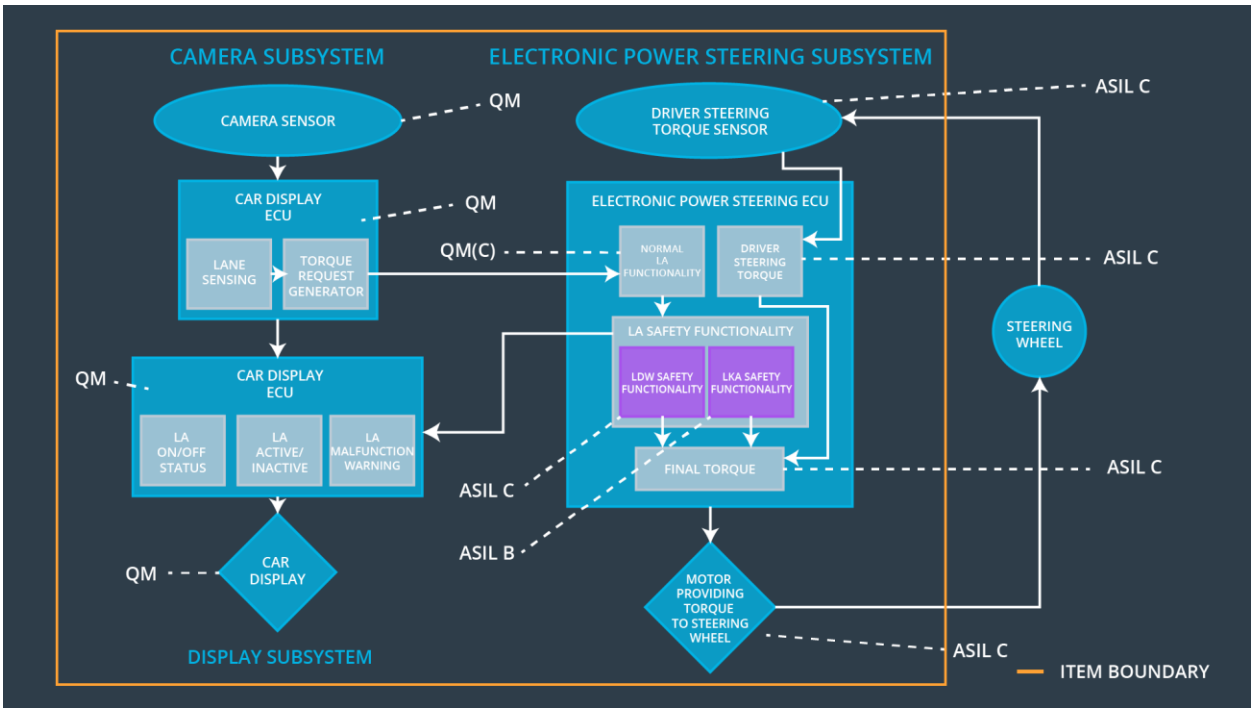

Figure 2

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 ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Vibrational torque request received by the Electronic Power Steering ECU is very high	Vibrational torque request is higher than MAX_Torque_Amplitude or MAX_Torque_Frequency	Yes	Display a malfunction warning light on the driver dashboard
WDC-02	Duration of the LKA torque request received by the electronic power steering ECU is long	Duration of torque request is more than Max_Duration	Yes	Display a malfunction warning light on the driver dashboard