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
2019.05.05	1.0	Chenglei Qiao	Initial revision

Table of Contents

Purpose of the Functional Safety Concept

In the functional safety concept phase, the high-level requirements of the system are identified. These requirements are allocated to different parts of 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 lane departure warning function shall be limited.
Safety_Goal_02	The lane keeping assistance 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 a autonomous driving.
Safety_Goal_03	The reaction time of the lane keeping assistance function shall not exceed a certain threshold.
Safety_Goal_04	Unexpected high oscillating torque shall be prevented.

Preliminary Architecture

The preliminary architecture for the lane assistance item is shown in figure 1.

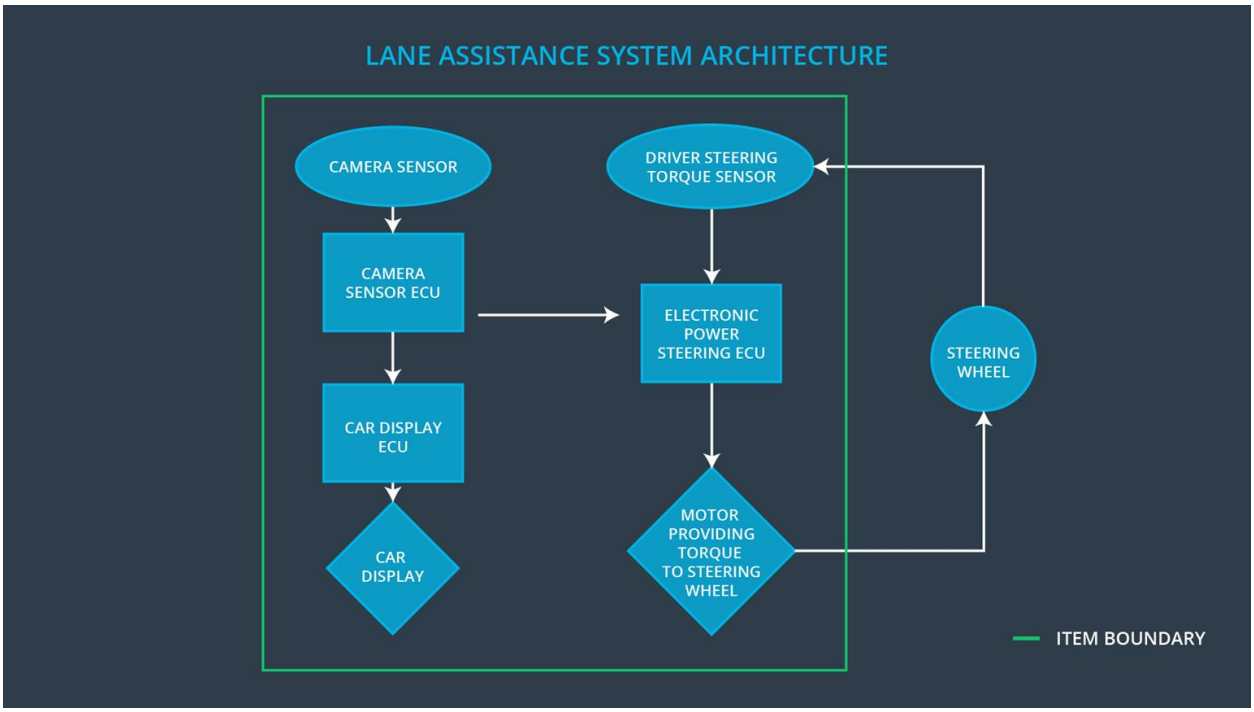

Figure 1 The preliminary architecture of the item

Description of architecture elements

Element	Description
Camera Sensor	Capture road images in front of the vehicle and provide to Camera Sensor ECU
Camera Sensor ECU	Calculate when the vehicle is leaving the lane Requests the EPS system to turn and vibrate the steering wheel Request the car display system to turn on warning light on dashboard
Car Display	Display warning and status lights for driver
Car Display ECU	Turn on warning and status lights on car display
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver
Electronic Power Steering ECU	Use the information received from the Driver Steering Torque Sensor and the torque requested by the Lane Keeping Assistance and Lane Warning and request the necessary torque to be applied by the Motor actuator.

Motor	Applies the torque indicated by the Electronic Power Steering ECU 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 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

[Instructions: Fill in the functional safety requirements for the lane departure warning]

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 LDW oscillating torque amplitude is below *Max_Torque_Amplitude*	C	50ms	Turn off LDW
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the LDW oscillating torque frequency is below *Max_Torque_Frequency*	C	50ms	Turn of LDW

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	Normal drivers can control the vehicle when torque amplitude is within *Max_Torque_Amplitude*	*Criterion*: When the torque amplitude crosses *Max_Torque_Amplitude*, the LA output is set to zero within 50 ms *Method:* Insert torque signal with amplitude greater than *Max_Torque_Amplitude*
Functional Safety Requirement 01-02	Normal drivers can control the vehicle when torque frequency is within *Max_Torque_Frequency*	*Criterion:* When the torque frequency crosses *Max_Torque_Frequency*, the LA output is set to zero within 50 ms *Method:* Insert torque signal with frequency greater than *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 assistance item shall ensure that the LKA torque is applied for only *Max_Duration*	B	500ms	Turn off LKA
Functional Safety Requirement 02-02	The lane assistance item shall ensure that the LKA torque amplitude is greater than *Min_Torque_Amplitude*	QM	500 ms	Turn off LKA

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 *Max_Duration* value chosen forces drivers not to take their hands off the steering wheel during driving	*Criterion:* When the LKA torque is applied for more than *Max_Duration* seconds, the LKA output is set to zero within 500 ms *Method:* Artificially inject torque request from LKA system lasting more than *Max_Duration* seconds
Functional Safety Requirement 02-02	The *Min_Torque_Amplitude* value chosen is adequate to physically steer the vehicle back to lane center each time there is deviation	*Criterion:* When the LKA torque applied is less than *Min_Torque_Amplitude*, the LKA output is set to zero within 500 ms *Method:* Artificially reduce LKA torque amplitude below *Min_Torque_Amplitude*

Refinement of the System Architecture

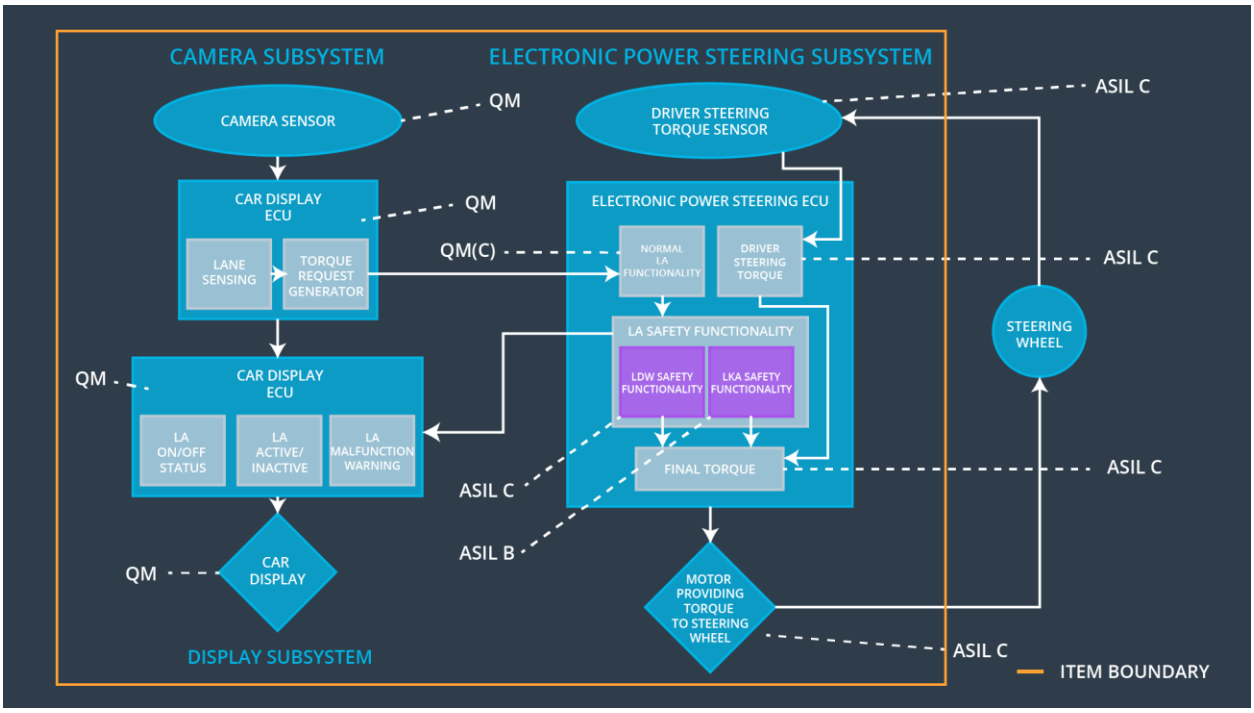

Figure 2 Refinement of the System Architecture

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 warning oscillating torque amplitude is below *Max_Torque_Amplitude*	**X**		
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the LDW oscillating torque frequency is below *Max_Torque_Frequency*	**X**		
Functional Safety	The EPS ECU shall ensure that the LKA torque is applied for only	**X**		

Requirement 02-01	*Max_Duration*			
Functional Safety Requirement 02-02	The EPS ECU shall ensure that the LKA torque amplitude is greater than *Min_Torque_Amplitude*	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW	Is_Max_Torque_ Exceeded	Yes	Warning light on car display
WDC-02	Turn off LKA	Is_Max_Duration _Exceeded	Yes	Warning light on car display