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
2018.10.29		Wanlin Yang	gandue

Table of Contents

Purpose of the Functional Safety Concept

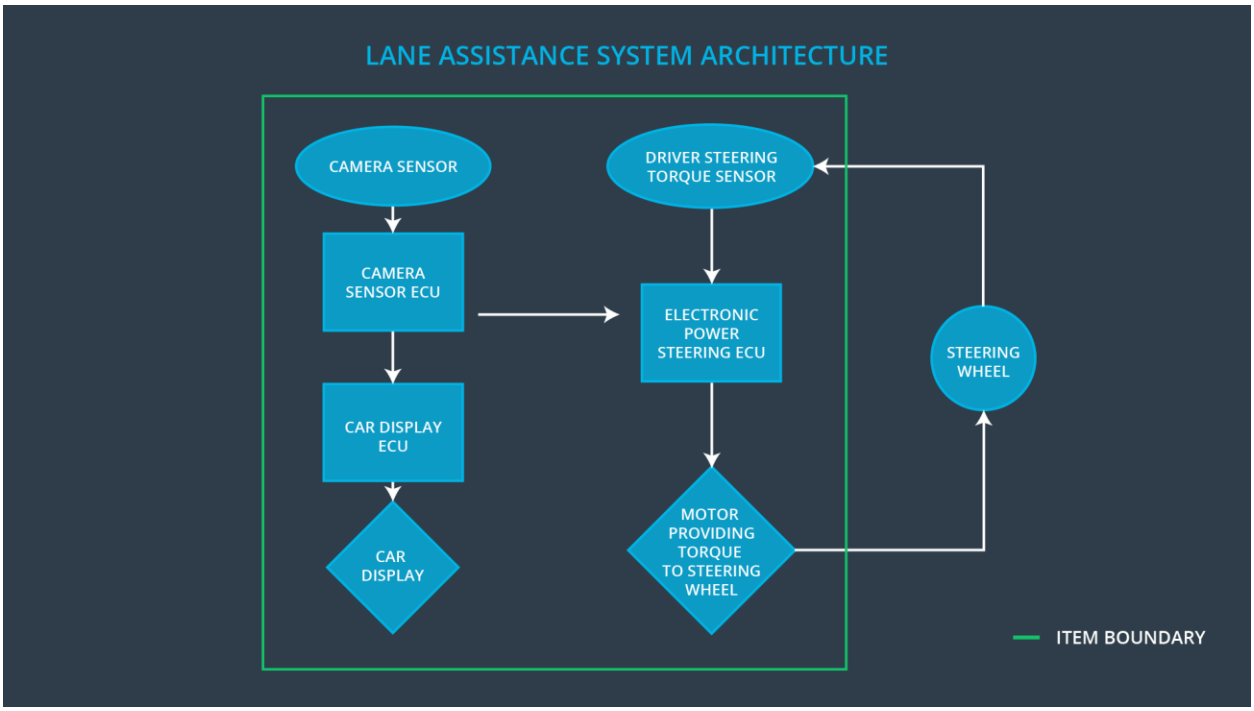
The functional safety concept provides a high level overview of the system. Based on the hazard analysis and risk assessment, the requirements of the system will be figured out in this section. The safety goals are refined into safety requirements. These safety requirements are then allocated to the appropriate parts of the item’s architecture.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating torque to the steering wheel from the lane departure 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 so that the driver cannot misuse the system for autonomous driving.

Preliminary Architecture



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 the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	The Car Display is the user interface that displays warning and suggestion on dashboard.
Car Display ECU	The Car Display ECU receives signal from the Camera Sensor ECU, processes image information, and sends output to the Car Display.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor measures how much the driver is turning, and sends data to the Electronic Power Steering ECU.
Electronic Power Steering ECU	The Electronic Power Steering ECU computes how hard the steering wheel should turn and vibrate based on car's departure information, and sends messages to the Motor.
Motor	Motor is the actuator that vibrates and turns 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

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 oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	LDW will set the oscillating torque amplitude to 0.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	LDW will set the oscillating torque frequency 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	Test how drivers react to different torque amplitudes to prove that the value is appropriate.	When the torque amplitude crosses the limit, the lane assistance output is set to zero within the fault tolerant time interval.
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that the value is appropriate.	When the torque frequency crosses the limit, the lane assistance output is set to zero within the fault tolerant time interval.

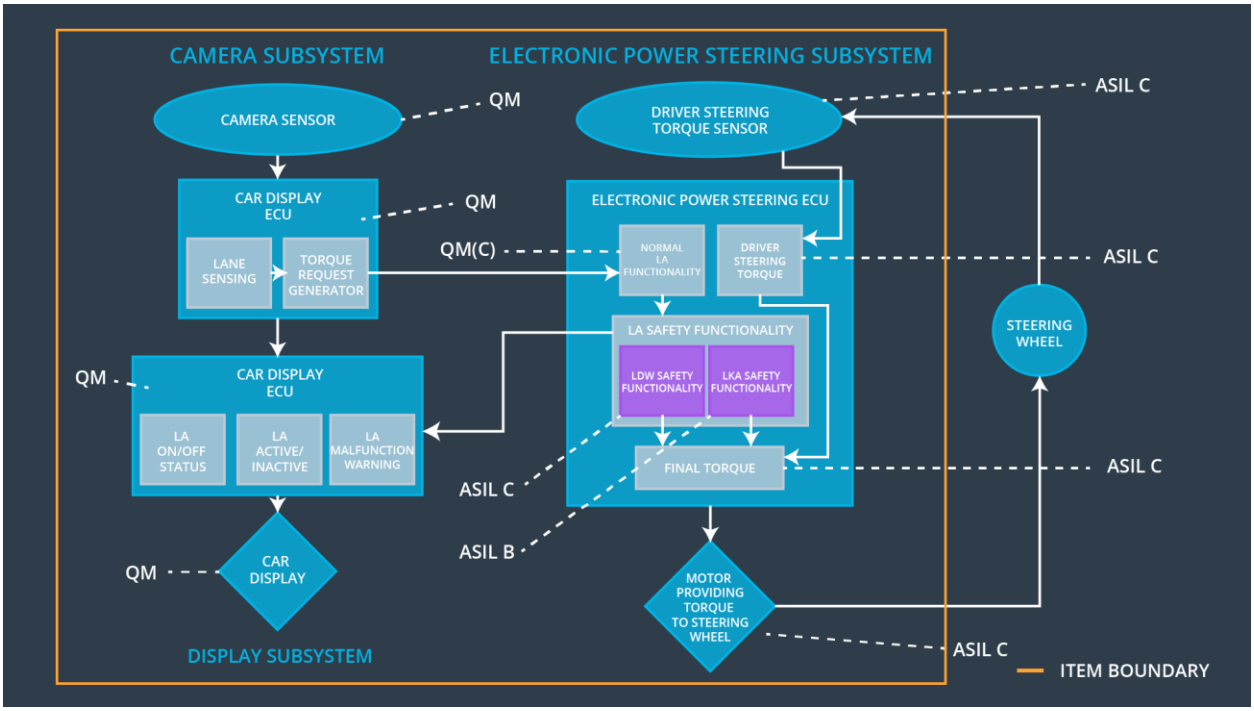
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	50 ms	The LKA will turn off the assistance 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	The Max_Duration really did dissuade drivers from taking their hands off the wheel.	The system really does turn off if the lane keeping assistance while exceeding 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 electronic power steering ECU shall ensure that the oscillating torque amplitude is below Max_Torque_Amplitude.	X		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the oscillating torque frequency is below Max_Torque_Frequency.	X		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	X		

Warning and Degradation Concept

[Instructions: Fill in the 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, Malfunction_04.	Yes	The warning is shown on the Car Display system.
WDC-02	Turn off the functionality.	Malfunction_03, Malfunction_05	Yes	The warning is shown on the Car Display system.