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
2017.09.14	1	Denise James	Initial Release
2017.09.28	2	Denise James	Changed Functional Safety Requirement 02-01 ASIL to “B”

Table of Contents

Document history

Table of Contents

Purpose of the Functional Safety Concept

Inputs to the Functional Safety Concept

- Safety goals from the Hazard Analysis and Risk Assessment
- Preliminary Architecture
  - Description of architecture elements

Functional Safety Concept

- Functional Safety Analysis
- Functional Safety Requirements
- Refinement of the System Architecture
- Allocation of Functional Safety Requirements to Architecture Elements
- Warning and Degradation Concept

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

The safety goals from the Hazard Analysis and Risk Assessment are shown in the table below.

ID	Safety Goal
Safety_Goal_01	Limit the torque applied to the steering wheel when the Lane Departure Warning function is always on.
Safety_Goal_02	The Lane Keep Assist function is time limited and the additional torque ends after a time when the LKA function is always on.
Safety_Goal_03	Alert the driver with audio and dashboard lights that the Lane Departure Warning function is not working.
Safety_Goal_04	Alert the driver with audio and dashboard lights that the Lane Keep Assist function is not working.

Preliminary Architecture

Figure 1 is an Overall Lane Assistance architecture diagram from the Udacity Lecture Notes[1]

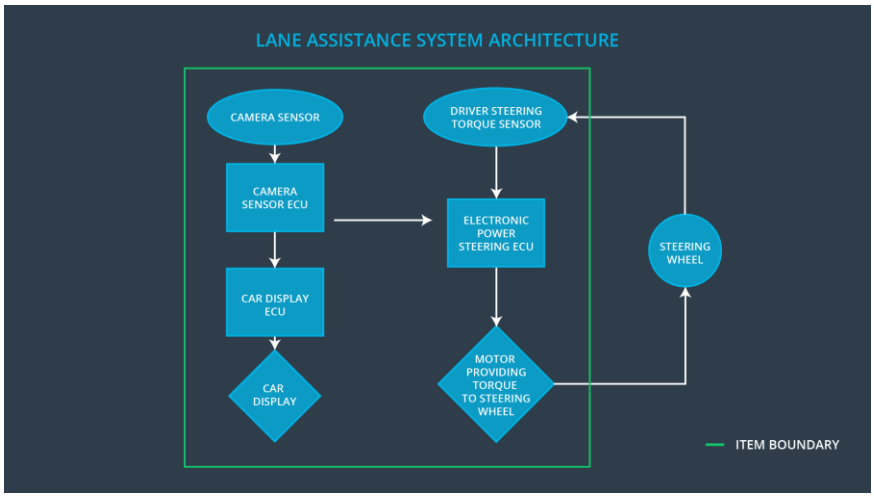


Figure 1

Description of architecture elements

Element	Description
Camera Sensor	A sensor that detects and conveys information that represents an image
Camera Sensor ECU	An electronic control unit that takes the camera sensor information and translates it to software data.
Car Display	Display in the car that takes data from the car display ECU and provides lighted icons and audio warnings sounds.
Car Display ECU	An electronic control unit that takes the camera sensor ECU output as an input. The output of the car display ECU is sent to the Car Display as an input.
Driver Steering Torque Sensor	A sensor that detects and measures the torque value . This value is sent to the Electronic Power Steering ECU as an analog signal.
Electronic Power Steering ECU	Takes in analog sensor measurements from the camera and driver steering torque sensor.
Motor	The motor receives power from the Electronic Power Steering ECU based on software settings. The motor provides 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 lane departure warning function applies an oscillating torque with very high torque amplitude (above MAX_TORQUE_AMP)
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 (MAX_TORQUE_FREQ)"
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 lane departure warning oscillating torque amplitude is below $Max\_Torque\_Amplitude_2$	C	50 ms	LDW function is turned off with a lighted icon on the car display
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque frequency is below $Max\_Torque\_Frequency_2$	C	50 ms	LDW function is turned off with a lighted icon on the car display

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 function with the max torque amplitude. Assure the LDW function is turned off at the max_torque_amplitude. Validate the functionality of the LDW function with valid torque_amplitude values.	Verify the LDW functions with values less than the max_torque_frequency. Verify the LDW function does turn off and display a lighted icon on the car display to let the driver know LDW is off.
Functional Safety Requirement 01-02	Test the LDW function with the max torque frequency. Assure the LDW function is turned off at the max_torque_frequency. Validate the functionality of the LDW function with valid torque_frequency values.	Verify the LDW functions with values less than the max_torque_frequency. Verify the LDW function does turn off and display a lighted icon on the car display to let the driver know LDW is off.

Lane Keeping Assistance (LKA) Requirements:

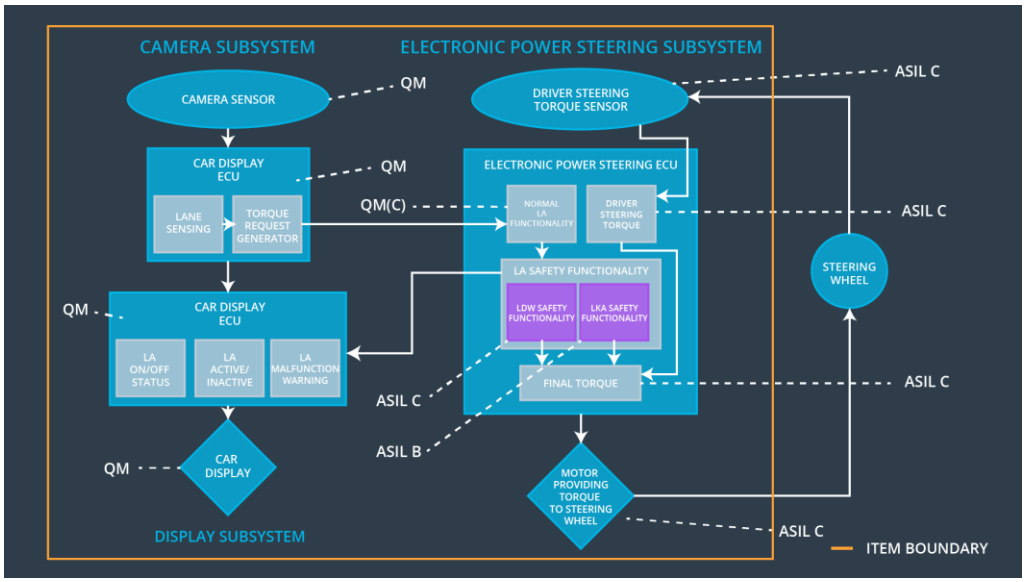
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	"The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration".	B	50 ms	LKA function is turned off with a lighted icon on the car display

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 function to validate that the Max_Duration time applied to the system shuts the LKA function off.	Verification is done by another party that the Max_Duration time applied to the system shuts the LKA function off.

Refinement of the System Architecture

Lane Assistance Architecture Refinement Diagram From Udacity Lecture Notes[x]



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 lane departure warning oscillating torque amplitude is below $Max\_Torque\_Amplitude_2$	X		
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque frequency is below $Max\_Torque\_Frequency_2$	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

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	LDW function is turned off with a lighted icon on the car display	Max_Torque_Amplitude or Max_Torque_Freq is higher	YES	Icon lighted on car display.
WDC-02	LKA function is turned off with a lighted icon on the car display	lane keeping assistance torque is applied for longer than Max_Duration	YES	Icon lighted on car display.