Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
2018-10-20	1.0	Rodrigo Vasconcelos	Initial version of the document
2018-10-22	2.0	Rodrigo Vasconcelos	Adjusted LDW and LKA Safe State to reflect that a better safe state (rather than turning the LA system off) is to set the output torque from the LA functions to zero.

Table of Contents

Purpose of the Functional Safety Concept

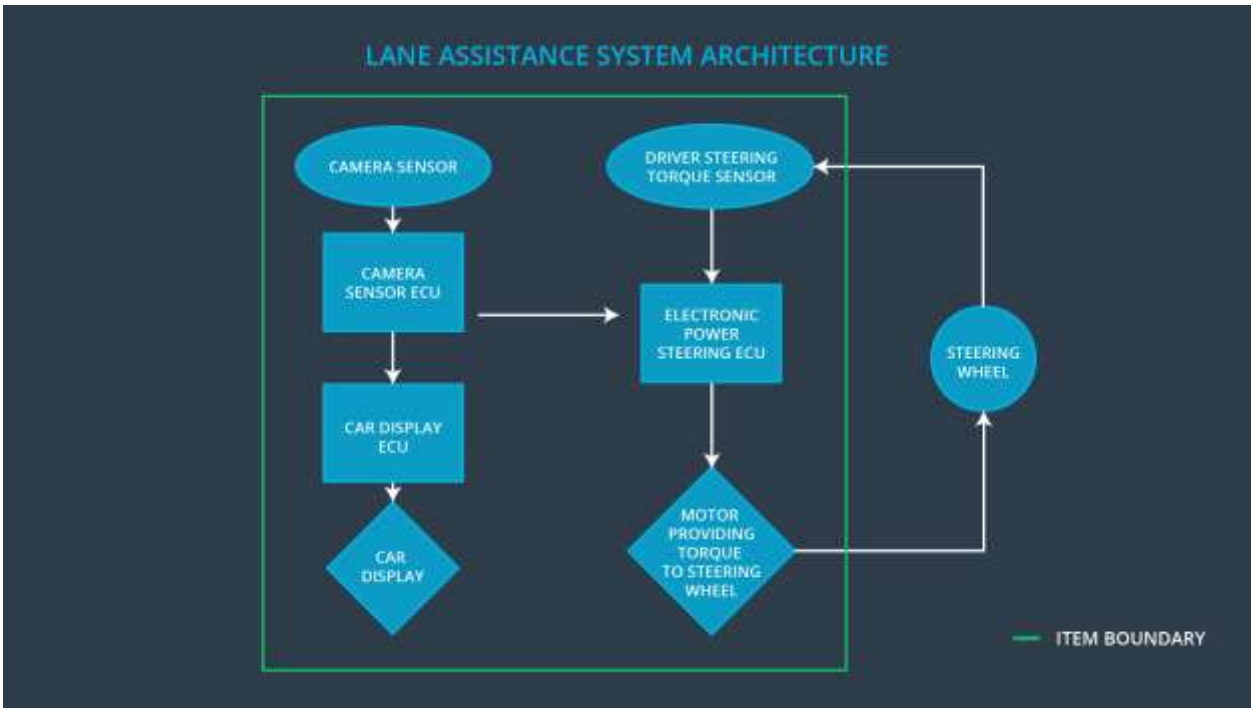
The purpose of this document is to allocate the Lane Assisting item’s safety requirements to an element of the system’s architecture in order to refine the system’s architecture and identify technical requirements.

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 autonomous driving.
Safety_Goal_03	The lane keeping assistance function shall apply the minimum torque necessary to return the car to the center of the lane.

Preliminary Architecture



Element	Description
Camera Sensor	Capture the scene in front of the car.
Camera Sensor ECU	Identify lane boundaries and the car's position relative to the center of the lane. Calculate the torque needed to return the car to the center of the lane.
Car Display	Display a light when the Lane Keeping function is on. Display a light when the Lane Assistance system is on. Display a light when the Lane Assistance system experiences a malfunction.
Car Display ECU	Interpret the Lane Assistance system state to enable the appropriate lights. Identify when the driver activates a turn signal. Identify when the driver disengages the Lane Assistance system.
Driver Steering Torque Sensor	Read the steering torque applied by the driver.

Electronic Power Steering ECU	Oscillate the steering wheel when the Lane Departure Warning is on. Apply the required torque to the steering wheel as indicated by the Camera Sensor ECU when the Lane Keeping function is on. Subtract the torque already applied by the driver to the total required to keep the car in the lane.
Motor	Apply the required 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 oscillating torque amplitude is too high.
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 oscillating torque frequency is too high.

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 has no time limit.
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	MORE	The lane keeping assistance function applies a torque that is too high.

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 lane assistance item shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Set LDW output torque to zero
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Set LDW output torque 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	Test how drivers react to different torque amplitudes to prove that we chose an appropriate value.	Test using a value over Max_Torque_Amplitude and verify that the system is turned off within 50 ms.

Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that we chose an appropriate value.	Test using a value over Max_Torque_Frequency and verify that the system is turned off within 50 ms.

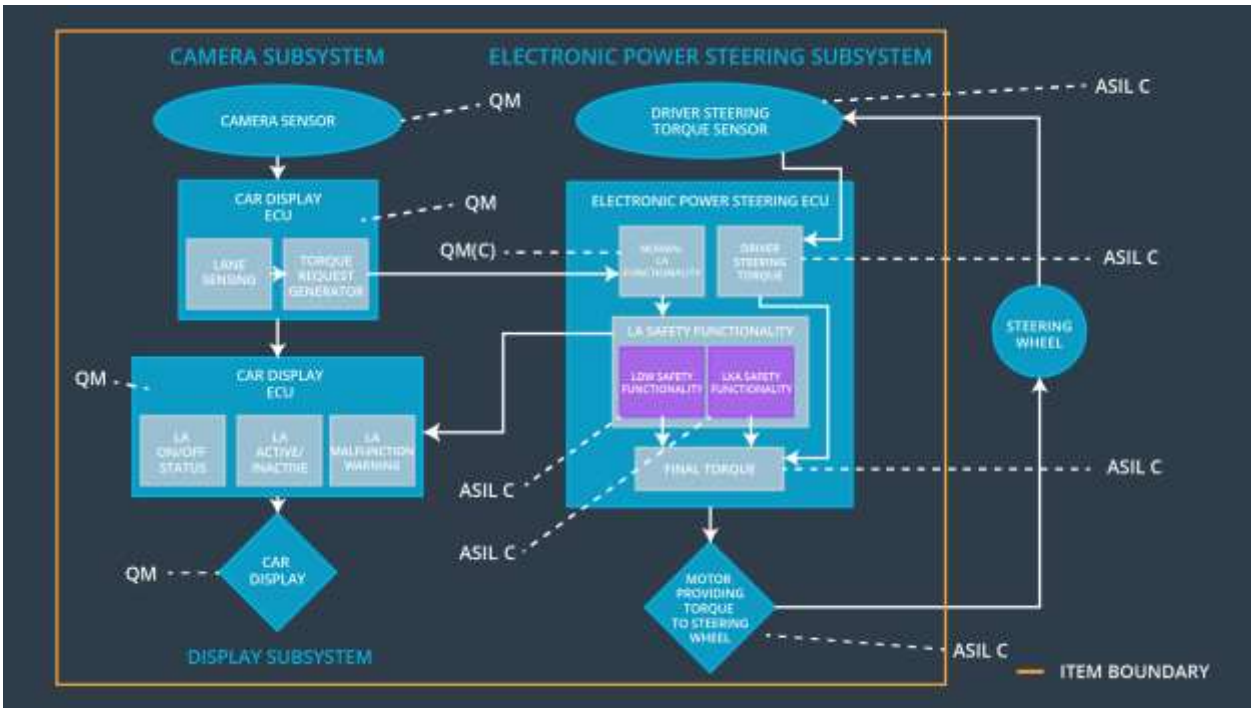
Lane Keeping Assistance (LKA) Requirements:

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	500ms	Set LKA output torque to zero
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque applied is not higher than Max_Torque_Amount	C	50ms	Set LKA output torque 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	Test times required to re-center the car under different conditions to prove that we chose an appropriate value.	Verify that the drivers are dissuaded from taking their hands off the steering wheel with the selected max duration.
Functional Safety Requirement 02-02	Test how drivers react to different torque magnitudes to prove that we chose an appropriate value.	Test using a value over Max_Torque_Magnitude and verify that the system is turned off within 50 ms.

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 lane departure warning 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**		
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque applied is not higher than Max_Torque_Amount	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the Lane Assistance item.	Steering oscillating amplitude is too high.	Yes	Display light on dashboard.
WDC-02	Turn off the Lane Assistance item.	Steering oscillating frequency is too high.	Yes	Display light on dashboard.
WDC-03	Turn off the Lane Assistance item.	The lane keeping assistance function is active for more than Max_Duration.	Yes	Display light on dashboard.
WDC-04	Turn off the Lane Assistance item.	The lane keeping assistance function applies a torque that is too high.	Yes	Display light on dashboard.