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
20/05/2018	1.0	Trijeet	Initial Draft

Table of Contents

Purpose of the Functional Safety Concept

The purpose of the functional safety concept is to identify the high level system requirements without diving deep into the technical aspects. Different parts of the item architecture are allocated with the responsibility of fulfilling these requirements. The result of this leads to construction of the technical safety requirements from it. Validation and verification instructions for these requirements are also laid down in this. Finally, these requirements will be considered while hardware and software implementation of the system.

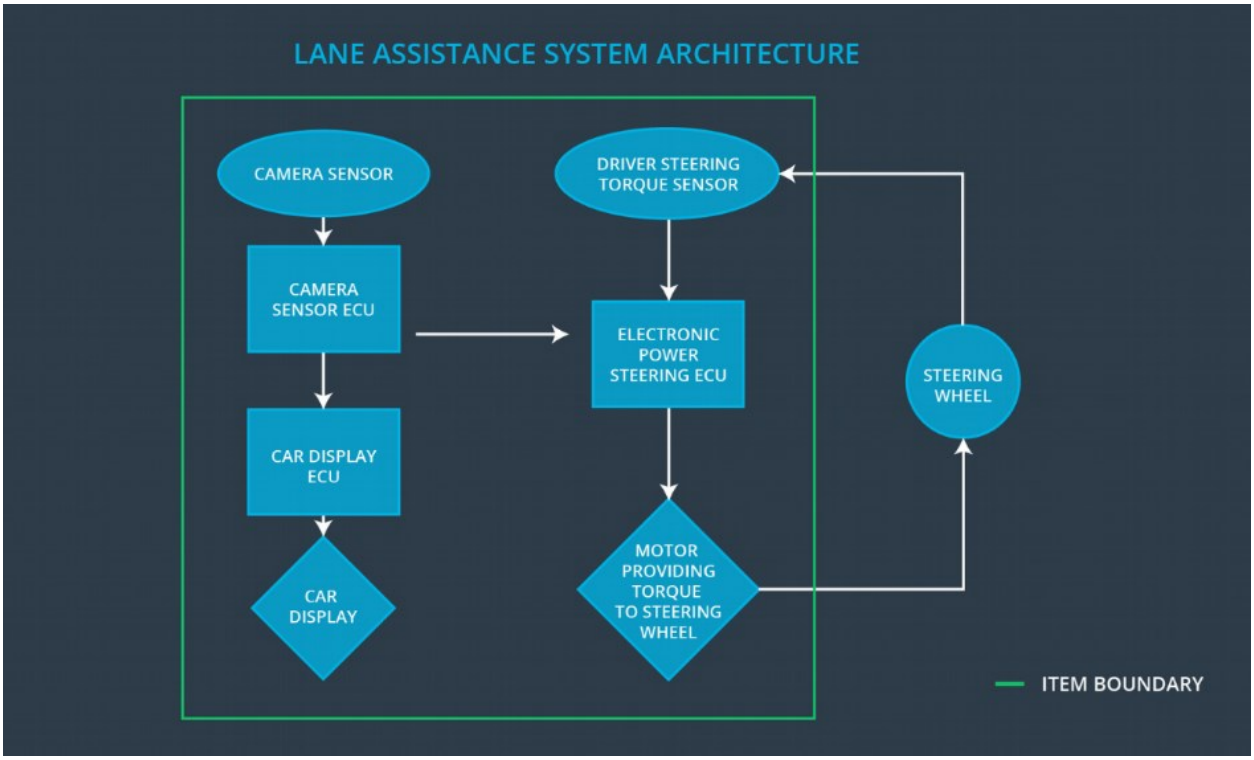
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the Lane Departure Warning shall be limited.
Safety_Goal_02	The Lane Keeping Assistance shall be time limited. 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 Departure Warning and the Lane Keeping Assistance shall be disabled as soon as the Camera sensors malfunction; followed by an alarm to notify the driver about this incident.

Preliminary Architecture

The architecture is depicted in the following image:



Description of architecture elements

Element	Description
Camera Sensor	Captures the scene in front of the car and feeds the image to the Camera Sensor ECU.
Camera Sensor ECU	Processes the image to detect the components in the image (such as lane lines) and computes the car's position on the lane.
Car Display	Notifies the driver with alerts, warnings and status messages from the Lane Departure Warning and Lane Keeping Assistance functions.
Car Display ECU	Controls the signals and content to be displayed on the car display depending on the feed from the Camera Sensor ECU.
Driver Steering Torque Sensor	Measures the torque that is currently being applied on the steering wheel by the driver.
Electronic Power Steering ECU	Computes the torque that is further required to keep the car on the center of the lane, based on the inputs from the Lane Departure Warning and Lane Keeping Assistance functions.
Motor	Actuates the torque on 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 cause a very high oscillating steering torque amplitude which exceeds max 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 cause a very high oscillating steering torque frequency which exceeds max 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 constrained in time limit which might lead 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	Lane Departure Warning function shall ensure that the lane departure oscillation torque amplitude stays below Max_Torque_Amplitude	C	50 ms	Oscillation torque amplitude maintained below Max_Torque_Amplitude
Functional Safety Requirement 01-02	Lane Departure Warning function shall ensure that the lane departure oscillation torque frequency stays below Max_Torque_Frequency	C	50 ms	Oscillation torque amplitude maintained below Max_Torque_Frequency
Functional Safety Requirement 01-03	Lane Departure Warning shall be disabled when the Camera Sensors malfunction.	C	10 ms	Function disabled

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	Check that the Max_Torque_Amplitude is enough for the driver to detect it while not losing of control over the car.	Check that the Lane Departure Warning is disabled once it exceeds Max_Torque_Amplitude
Functional Safety Requirement 01-02	Check that the Max_Torque_Frequency is enough for the driver to detect it while not losing control over the car.	Check that the Lane Departure Warning is disabled once it exceeds Max_Torque_Frequency
Functional Safety Requirement 01-03	Check that the Camera Sensors are working correctly.	Check that the Lane Departure Warning is disabled as soon a Camera Sensors malfunction is detected.

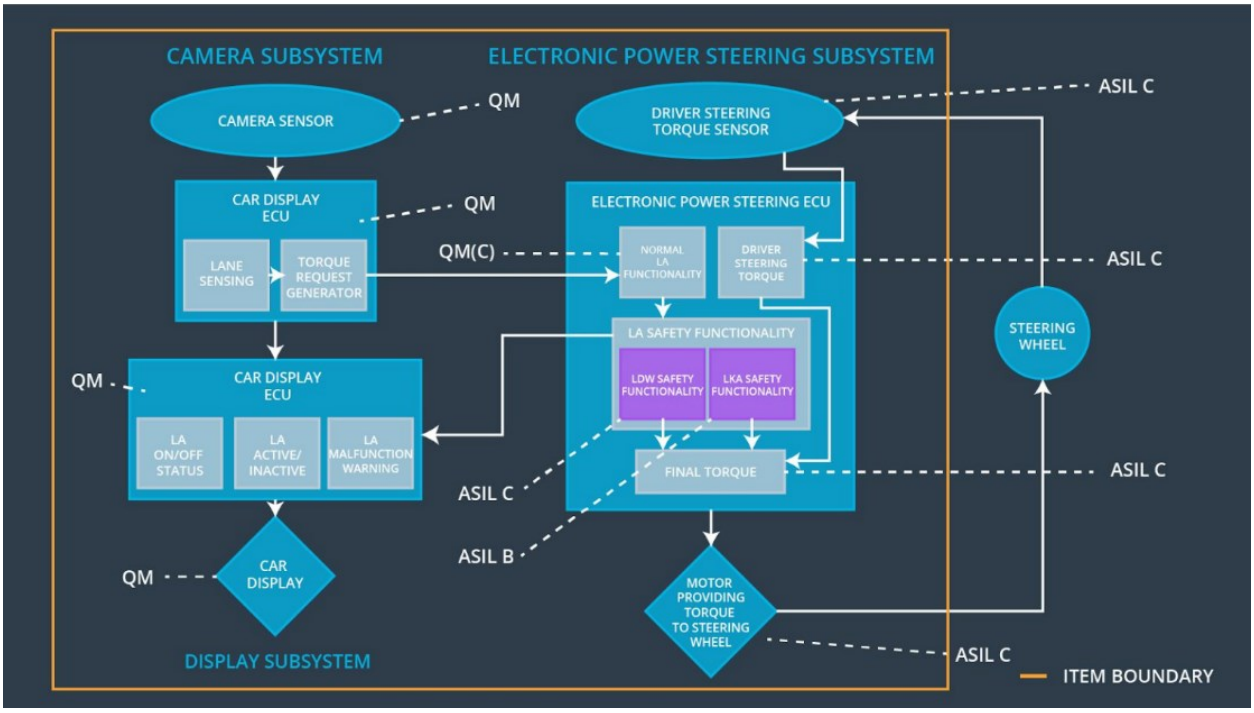
Lane Keeping Assistance (LKA) Requirements:

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 no more than Max_Duration	B	500 ms	Turn off the lane keeping assistance function
Functional Safety Requirement 02-02	The lane keeping assistance shall be deactivated when the electronic power steering ECU detects a camera malfunction.	C	10 ms	Function disabled

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	Check that the Max_Duration is chosen such that the driver disengage himself from autonomous driving.	Check that the system is disabled as and when the lane keeping assistance torque is applied for a duration that exceeds Max_Duration.
Functional Safety Requirement 02-02	Check that the lane keeping assistance whenever there is a malfunction in the camera sensors	Check that lane keeping assistance is disabled as soon a camera malfunction is detected.

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 keeping assistance function shall ensure that the lane departure oscillation torque amplitude stays below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The lane keeping assistance function shall ensure that the lane departure oscillation torque frequency stays below Max_Torque_Frequency	**X**		
Functional Safety Requirement 01-03	Lane departure warning shall be disabled when the camera sensors malfunction.	**X**		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for no more than Max_Duration	**X**		
Functional Safety Requirement 02-02	The lane keeping assistance shall be deactivated when the electronic power steering ECU detects a camera malfunction.	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Disable lane departure warning	Malfunction_01, Malfunction_02	Yes	Alert on car display: Lane Departure Warning Malfunction
WDC-02	Disable lane keeping assistance	Malfunction_03	Yes	Alert on car display: Lane Keeping Assistance Malfunction