Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-03-26	1.0	Felipe A. L. Reis	First submission.

Table of Contents

Purpose of the Functional Safety Concept

Functional safety has the major purpose to reduce risks to acceptable levels, avoiding accidents. Functional safety contains some safety requirements that must be done to achieve it's major purpose.

Functional safety is also part of ISO 26262 requirements and also one of the documents to guarantee the safe management.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

The goal of this document is provide a hazard analysis and risk assessment to predict and identify possible problems that can cause accidents and lead to an injury. The major objective is to reduce the risk to acceptable levels, tolerated by society.

ID	Safety Goal
Safety_Goal_01	"The lane keep item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude" [1].
Safety_Goal_02	"The lane keep item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency" [1].

Table 1. Safety goals

Preliminary Architecture

The preliminary Lane Assistance System Architecture is defined in Image 1. As shown in Image 1, the Item boundary contains three subsystems:

- Camera system *(Camera Sensor ECU);*
- Car Display System *(Car Display ECU);*
- Electronic Power Steering System *(Electronic Power Steering ECU).*

Outside Item boundary is some system like wheel, throttle and other components of the vehicle.

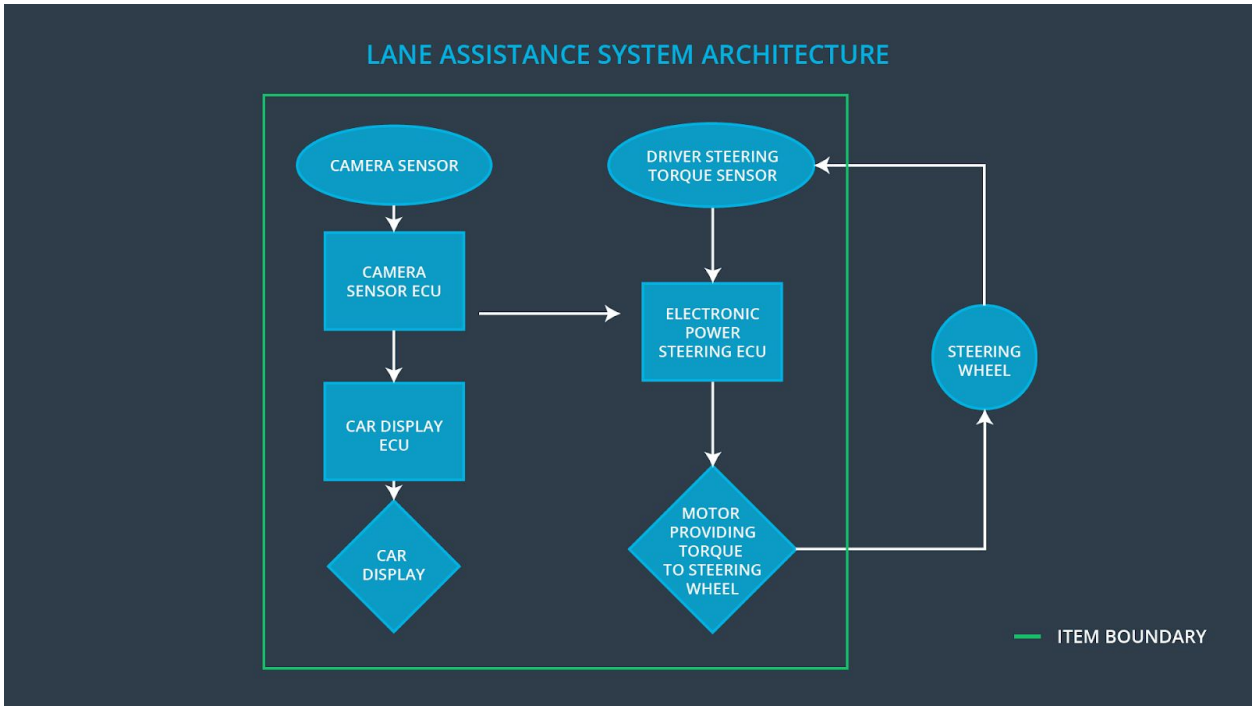

Image 1. Preliminary Lane Assistance System Architecture

Description of architecture elements

Element	Description
Camera Sensor	Responsible for detect lane lines (using optical detection).
Camera Sensor ECU	ECU (Electronic Control Unit) is responsible to retrieve data from camera sensor and process its information. If the ECU identifies the vehicle leaving the lane, it is its responsibility to send a signal to start LKA and LDW functions.
Car Display	Responsible for indicate the driver the current usage of the system.
Car Display ECU	Responsible for receive and process signal from Camera Sensor ECU and determine if the display must show a visible information to the driver.
Driver Steering Torque Sensor	Responsible for identify the torque applied by the driver to correct the trajectory.
Electronic Power Steering ECU	Responsible for receive data from Camera Sensor ECU and Driver Steering Torque Sensor and determine the correct extra torque that should be applied by motor to correct the trajectory with the best way possible. Also responsible to vibrate the steering wheel, indicating the driver that the system is working right now.

Motor	Responsible for add an extra torque to correct the trajectory.

Table 2. Architecture elements

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	LDW applies a torque with higher amplitude than recommended causing difficult to the driver control the car.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	LESS	LDW applies a torque so small, not perceived by the driver, that can't see that the car is leaving the lane.
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	LDW works but LKA don't, misleading the driver.

Table 3. Malfunctions

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Req. 01-01	“The lane keep item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude” [1].	C	50 ms	Set the vibration torque to zero.
Functional Safety Req. 01-02	“The lane keep item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency” [1].	C	50 ms	Set the vibration torque to zero.

Table 4. LDW Requirements

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Req. 01-01	Some tests may be set to view the driver's reaction for different torque amplitudes. The results must be between a tested min and a max limit.	Verify if the system amplitude is really between min and max allowed amplitudes, ensuring a comfort and an alert vibration.
Functional Safety Req. 01-02	Some tests may be set to view the driver's reaction for different torque frequencies. The results must be between a tested min and a max limit.	Verify if the system amplitude is really between min and max allowed frequencies, ensuring a comfort and an alert vibration.

Table 5. LDW Verification and Validation Acceptance Criteria

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Req. 02-01	System should not performance any assistance above the Max_Duration, defined only to keep the vehicle in the lane.	B	500ms	The extra torque should be set to zero.

Table 6. LKA Requirements

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Req. 02-01	Verify the average time to set the car back to lane and add an extra tolerance, defining the Max_Duration time.	LKA should not work more than Max_Duration time, prevent the driver to take his hands out of the steering wheel.

Table 7. LKA Verification and Validation Acceptance Criteria

Refinement of the System Architecture

The refined Lane Assistance System Architecture is defined in Image 2. As shown in Image 2, the Electronic Power Steering ECU take much more responsibilities when compared to the preliminar Lane Assistance System Architecture, in Image 1.

The refined system architecture contains some tests to identify integrity of the data, safety tests and other resources to prevent failures. Also, this architecture contains some information about the risks ASIL, derived from each part of the system.

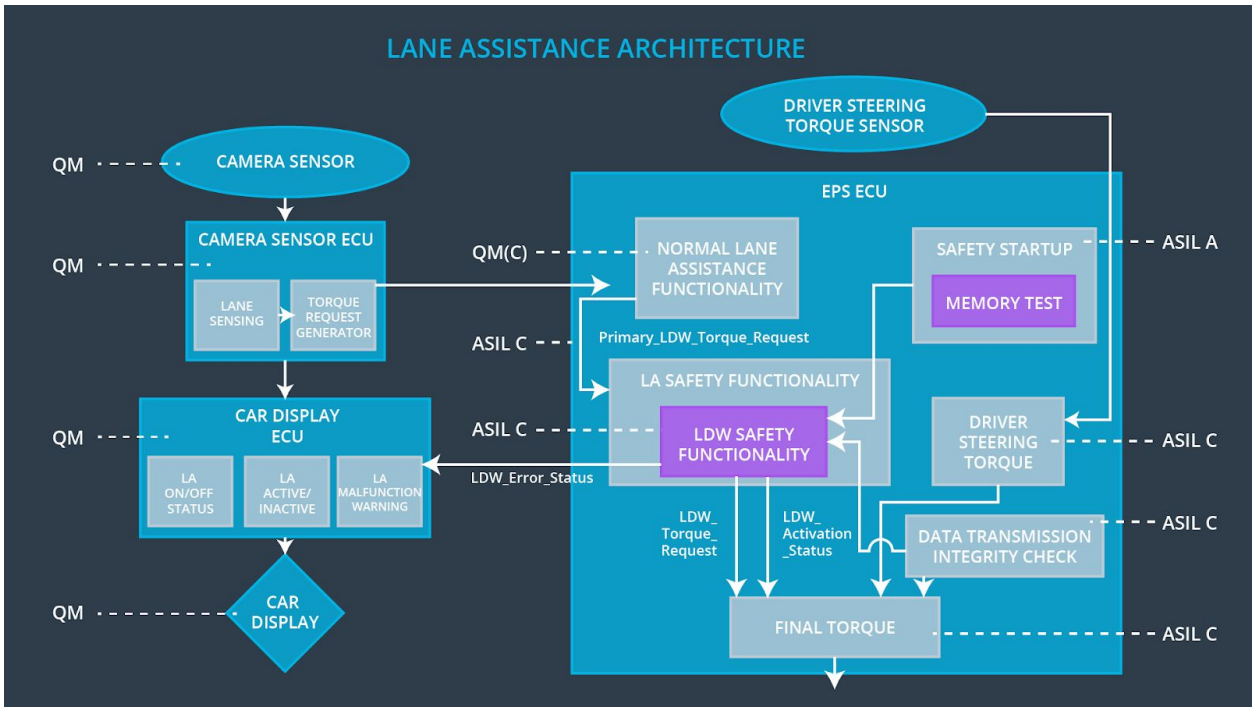

Image 2. Refined Lane Assistance System Architecture

Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Req. 01-01	“The lane keep item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude” [1].	**YES**	**NO**	**NO**
Functional Safety Req. 01-02	“The lane keep item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency” [1].	**YES**	**NO**	**NO**
Functional Safety Req. 02-01	The lane keep item shall ensure that the lane keep assistance do not work more than Max_Duration	**YES**	**NO**	**NO**

Table 8. Functional Safety Requirements and Allocation of Elements

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the functionality.	System working more time than allowed by Max_Duration time.	NO	Warning light.
WDC-02	Turn off the functionality.	Steering wheel torque is above Max_Frequency or Max_Amplitude limits.	YES	Warning light.

Table 9. Warning and Degradation

References

[1] Functional Safety: Functional Safety Requirements. **Udacity**. Available in: https://classroom.udacity.com/nanodegrees/nd013/parts/6047fe34-d93c-4f50-8336-b70ef10cb4b2/modules/6dc3d743-2b0f-4ae6-97b7-e2ff866f17ef/lessons/77ba6d2d-fd67-4ed3-96ba-128120ca25c7/concepts/c5ad8ba4-2d9d-44b6-bede-d7dd3aef381a. Accessed in 2018-03-26.