Elektrobit

UDACITY

Technical 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 Technical Safety Concept

Technical safety has the purpose to transform functional safety requirements into technical requirements, a concrete number of specifications to develop hardware and software. Technical safety details the steps to achieve the reduction of risks into a acceptable level.

Inputs to the Technical Safety Concept

Functional Safety 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	50ms	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	50ms	Set the vibration torque to zero.
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 1. Functional Safety Requirements

Refined System Architecture from Functional Safety Concept

The refined Lane Assistance System Architecture is defined 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.

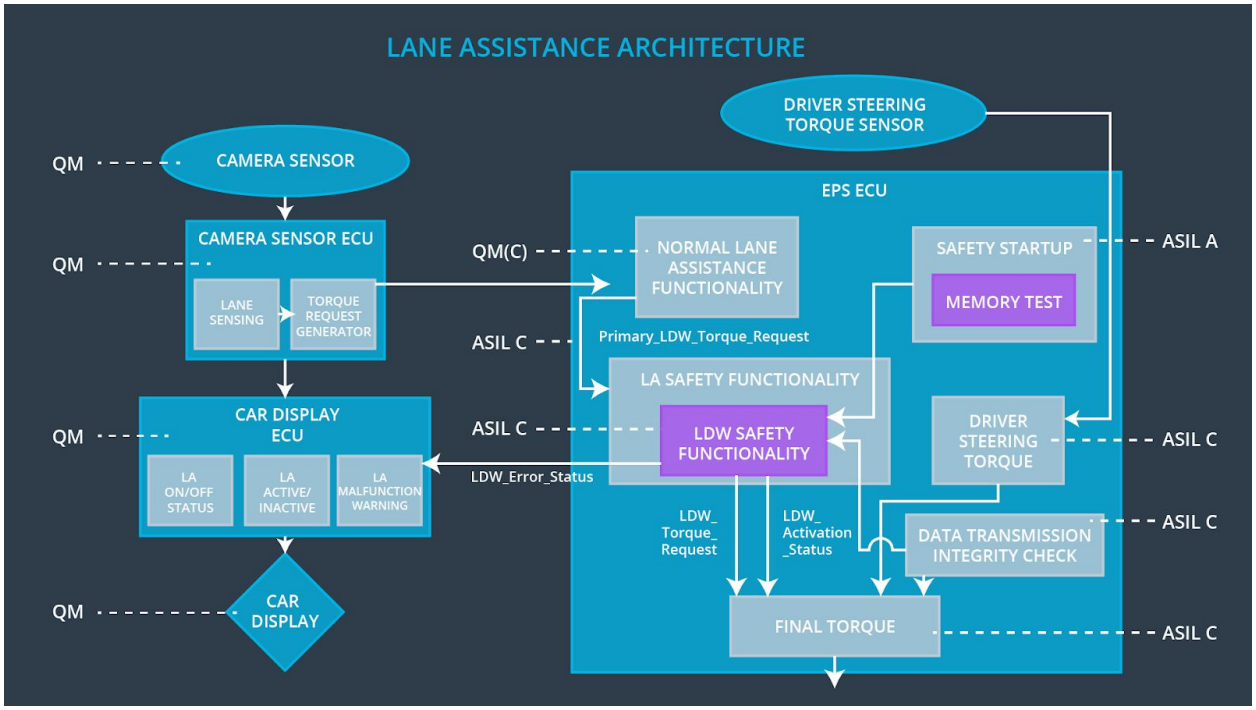

Image 1. Refined Lane Assistance System Architecture

Functional overview of architecture elements

Element	Description
Camera Sensor	Responsible for detect lane lines (using optical detection).
Camera Sensor ECU - Lane Sensing	Responsible for retrieve data from camera sensor and process its information. If the ECU identifies the vehicle leaving the lane. If the vehicle is leaving the lane, this ECU sends a signal to the Camera Sensor ECU - Torque request generator.
Camera Sensor ECU - Torque request generator	Responsible for send a signal to start LKA and LDW functions, in the Electronic Power Steering ECU.
Car Display	Responsible for indicate the driver the current usage of the system.
Car Display ECU - Lane Assistance On/Off Status	ECU responsible for recognize and show the information of ON/OFF to the driver.
Car Display ECU - Lane Assistant Active/Inactive	ECU responsible for show the information of activation or inactivation of the system to the driver.
Car Display ECU - Lane	ECU responsible to show the information of activation or

Assistance malfunction warning	inactivation of the system to the driver.
Driver Steering Torque Sensor	Responsible for identify the torque applied by the driver to correct the trajectory.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Responsible for receive data Driver Steering Torque Sensor, process it and sends a signal to the Final Torque ECU.
EPS ECU - Normal Lane Assistance Functionality	Responsible for receive data from Camera Sensor ECU, process it and sends a signal to the Final Torque ECU.
EPS ECU - Lane Departure Warning Safety Functionality	Responsible for keep the oscillating torque of the steering wheel below Max_Torque_Amplitude and Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Responsible for keep the LKA function working less time than Max_Duration.
EPS ECU - Final Torque	Responsible for receive data from Normal Lane Assistance Functionality ECU and Driver Steering Torque ECU and determine the correct extra torque that should be applied by motor to correct the trajectory with the best way possible.
Motor	Responsible for add an extra torque to correct the trajectory.

Table 2. Refined System Architecture from Functional Safety Concept

Technical Safety Concept

Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 with its associated system elements.

ID	Functional Safety Requirement	Electronic Power Steer. ECU	Camera ECU	Car Display ECU
Functional Safety Req. 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	X		

Table 3. Lane Departure Warning - Functional Requirements

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Req. 01	“The LDW component shall ensure the amplitude of ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering torque’ component is below ‘Max_Torque_Amplitude” [2]	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.
Technical Safety Req. 02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.
Technical Safety Req. 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.
Technical Safety Req. 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity	Set the vibration torque to zero.
Technical Safety Req. 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Check Integrity	Set the vibration torque to zero.

Table 4. Lane Departure Warning - Technical Requirements

Functional Safety Requirement 01-2 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU

Functional Safety Req. 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		

Table 5. Lane Departure Warning - Functional Requirements

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Req. 01	“The LDW component shall ensure the frequency of ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering torque’ component is below ‘Max_Torque_Frequency”	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.
Technical Safety Req. 02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.
Technical Safety Req. 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.
Technical Safety Req. 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity	Set the vibration torque to zero.
Technical Safety Req. 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Check Integrity	Set the vibration torque to zero.

Table 6. Lane Departure Warning - Technical Requirements

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Req. 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

Table 7. Lane Keeping Assistance - Functional Requirements

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Req. 01	“The LKA component shall ensure the duration of ‘LKA_Torque_Request’ sent to the ‘Final EPS torque’ not continue over Max_Duration time period.	C	500ms	EPS ECU - Lane Keeping Assistant Safety Functionality	Set torque to zero.
Technical Safety Req. 02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.	C	500ms	EPS ECU - Lane Keeping Assistant Safety Functionality	Set torque to zero.
Technical Safety Req. 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	500ms	EPS ECU - Lane Keeping Assistant Safety Functionality	Set torque to zero.
Technical Safety Req. 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	500ms	Data Transmission Integrity	Turn off functionality
Technical Safety	Memory test shall be conducted at start up of the EPS ECU to check	A	Ignition cycle	Memory Check Integrity	Turn off functionality

Req. 05	for any faults in memory.				

Table 8. Lane Keeping Assistance - Technical Requirements

Refinement of the System Architecture

The refinement of the Lane Assistance System Architecture is shown in Image 2. The refined system architecture contains extra safety checks that is unavailable in Image 1. This safety checks guarantee a correct transmission integrity and verify memory before start the module.

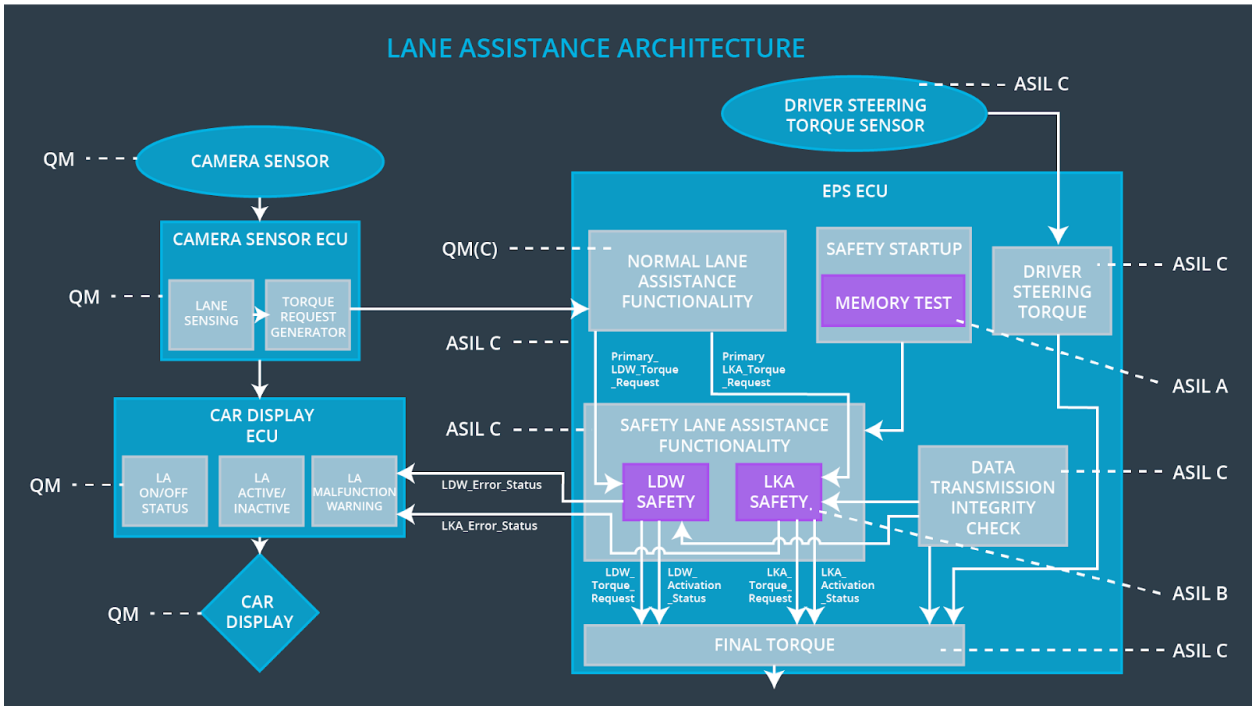

Image 2. Refinement of the Lane Assistance System Architecture

Allocation of Technical Safety Requirements to Architecture Elements

The technical safety requirements are allocated to the Electronic Power Steering ECU, in Technical Concept section.

Warning and Degradation Concept

Warning and degradation requirements are the same as the functional safety requirements. The requirements are detailed below.

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.

[2] Functional Safety: Deriving Technical Safety Requirements. **Udacity**. Available in: https://classroom.udacity.com/nanodegrees/nd013/parts/6047fe34-d93c-4f50-8336-b70ef10cb4b2/modules/6dc3d743-2b0f-4ae6-97b7-e2ff866f17ef/lessons/9734ccc4-75e5-4f7f-9f1f-483355714308/concepts/789309bf-c4f0-4a17-ae81-cc26d0fc6709. Accessed in 2018-03-27.

[3] Functional Safety: Technical Safety Requirements Attributes. **Udacity**. Available in: https://classroom.udacity.com/nanodegrees/nd013/parts/6047fe34-d93c-4f50-8336-b70ef10cb4b2/modules/6dc3d743-2b0f-4ae6-97b7-e2ff866f17ef/lessons/9734ccc4-75e5-4f7f-9f1f-483355714308/concepts/a0bad613-4bfa-4ecf-b712-337b56ef4e8e. Accessed in 2018-03-27.