Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
23rd May, 2019	1.0	Microsoft Word	Initial Version

Table of Contents

Purpose of the Technical Safety Concept

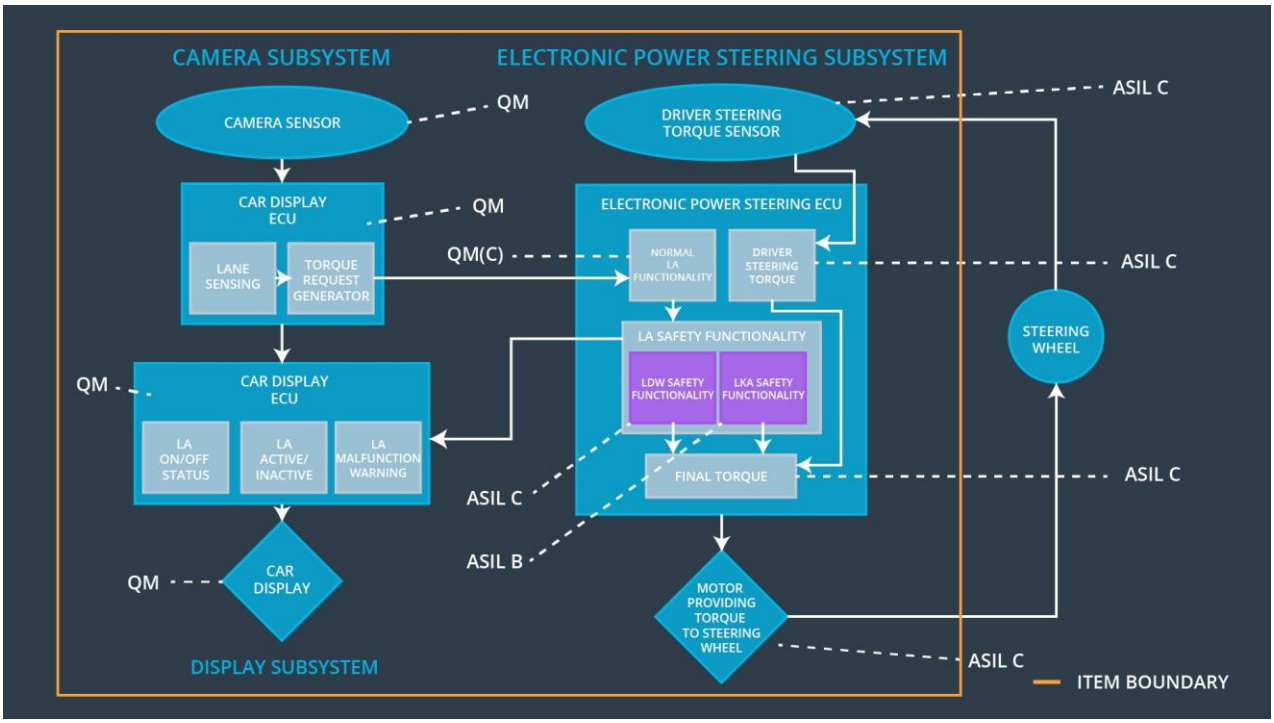
A technical safety concept is similar to a functional safety concept in the sense that it defines requirements and allocates them to subsystems. While a functional safety concept provides a bird’s eye view of the system, a technical safety concept goes deeper into the technical details of the system. Technical safety requirements are derived from functional safety requirements.

Inputs to the Technical Safety Concept

Functional Safety 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	C	50ms	Lane Departure warning function is not activated
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	C	50ms	Lane Departure warning function is not activated
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	Lane Keeping assistance system is not activated

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Perceives the environment through images which are passed to the camera sensor ECU for processing
Camera Sensor ECU - Lane Sensing	Determines if the car is leaving the lane and if so, determines the torque to be sent to the torque request generator
Camera Sensor ECU - Torque request generator	Sends a vibrational torque request to the power steering ECU
Car Display	Displays a number of visual cues that help the driver understand what the car is doing
Car Display ECU - Lane Assistance On/Off Status	Receives a signal from the power steering ECU about the status of the lane departure warning function and conveys the same to the display
Car Display ECU - Lane Assistant Active/Inactive	Receives a signal from the power steering ECU about the status of the lane assistance function and conveys the same to the display

Car Display ECU - Lane Assistance malfunction warning	Receives a signal from the power steering ECU if there is a malfunction with the lane assistance system and conveys the same to the display
Driver Steering Torque Sensor	Senses how much torque is already being applied by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Determines how much torque is already being applied by the driver
EPS ECU - Normal Lane Assistance Functionality	Receives the vibrational torque request from the camera ECU
EPS ECU - Lane Departure Warning Safety Functionality	Receives the request from the camera subsystem to activate/deactivate the lane departure warning system(i.e. to cause vibrations of the steering wheel) and conveys this request to the steering wheel through the motor
EPS ECU - Lane Keeping Assistant Safety Functionality	Receives the request from the camera subsystem to activate/deactivate the lane assistance system(i.e. to apply additional torque to the steering wheel) and conveys this request to the steering wheel through the motor
EPS ECU - Final Torque	Computes the final torque needed to be applied to the steering wheel after taking into consideration the torque already being applied by the driver and the torque requested by the camera subsystem and conveys the same to the motor
Motor	Applies the final torque to the steering wheel

Technical Safety Concept

Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 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 Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	X		

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 Requirement 01	LDW safety component shall ensure that the amplitude of the *LDW_torque_request* sent to the *Final Electronic Power Steering Torque* component is	C	50ms	LDW Safety Block	
	below Max_torque_amplitude				
Technical Safety Requirement 02	Validity and Integrity of the data transmission for the *LDW_Torque_Request* signal shall be ensured	C	50ms	Data Transmission Integrity Check	The lane departure warning torque request amplitude shall be set to zero
Technical Safety Requirement 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	LDW Safety Block	
Technical Safety Requirement 04	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	C	50ms	LDW Safety Block	
	warning light.				
Technical Safety Requirem	Memory test shall be conducted at the startup of EPS ECU to	A	Ignition cycle	Separate External block with Memory	
ent 05	check for any faults in memory.			test code	

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 Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		

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 Requirement 01	LDW safety component shall ensure that the frequency of the *LDW_torque_request* sent to the *Final Electronic Power Steering*	C	50ms	LDW Safety Component	The lane departure warning torque request amplitude shall be set to zero
	Torque component is below				
	Max_torque_frequency				
Technical Safety Requirement 02	Validity and Integrity of the data transmission for the *LDW_Torque_Request* signal shall be ensured	C	50ms	Data Transmission Integrity Check	
Technical Safety Requirement 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	C	50ms	LDW Safety Component	
	to zero.				
Technical	As soon as the LDW function	C	50ms	LDW Safety	

Safety Requirement 04	deactivates the LDW feature, the LDW safety software block shall send a signal to the car display ECU to turn on a warning light.			Component	
Technical Safety Requirement 05	Memory test shall be conducted at the startup of EPS ECU to check for any faults in memory.	A	Iginition Cycle	Separate External block with Memory test code	

Lane Keeping Assistance (LKA) Requirements:

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

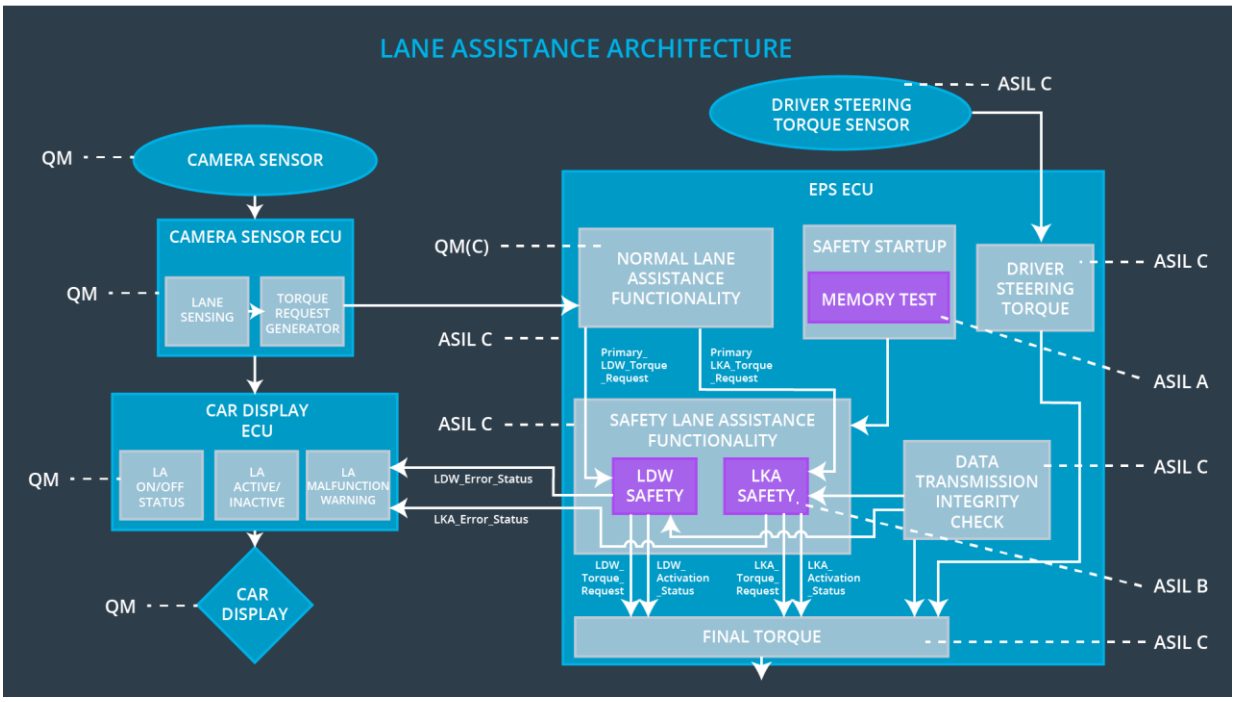
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 Requireme nt 01	LKA safety component shall ensure that the duration of the *LKA_torque_request* sent to the *Final Electronic Power Steering Torque* component is below	B	500ms	LKA safety component	
	Max_torque_duration				
Technical Safety Requireme nt 02	Validity and Integrity of the data transmission for the *LKA_Torque_Request* signal shall be ensured	B	500ms	Data Transmission Integrity Check	The lane

Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the *LKA_Torque_Request* shall be set to zero.	B	500ms	LKA safety component	departure warning torque request amplitude shall be set to zero
Technical Safety Requirement 04	As soon as the LKA function deactivates the LKA feature, the LKA safety software block shall send a signal to the car display ECU to turn on a warning light.	B	500ms	LKA safety component	
Technical Safety Requirement 05	Memory test shall be conducted at the startup of EPS ECU to check for any faults in memory.	A	Ignition Cycle	Separate External block with Memory test code	

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

Ror this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU

Warning and Degradation Concept

The warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements.
In both the cases(Lane Departure Warning and Lane Keeping Assistance):

Warning	Warning light displayed to the driver on the dashboard
Degradation	Turn off functionality