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
21/6/2018	1.0	Aditya	

Table of Contents

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to refine the functional safety requirements established in the functional safety concept into technical safety requirements. This is a crucial step before developing reliable hardware and software. As part of product development technical safety concept involves:

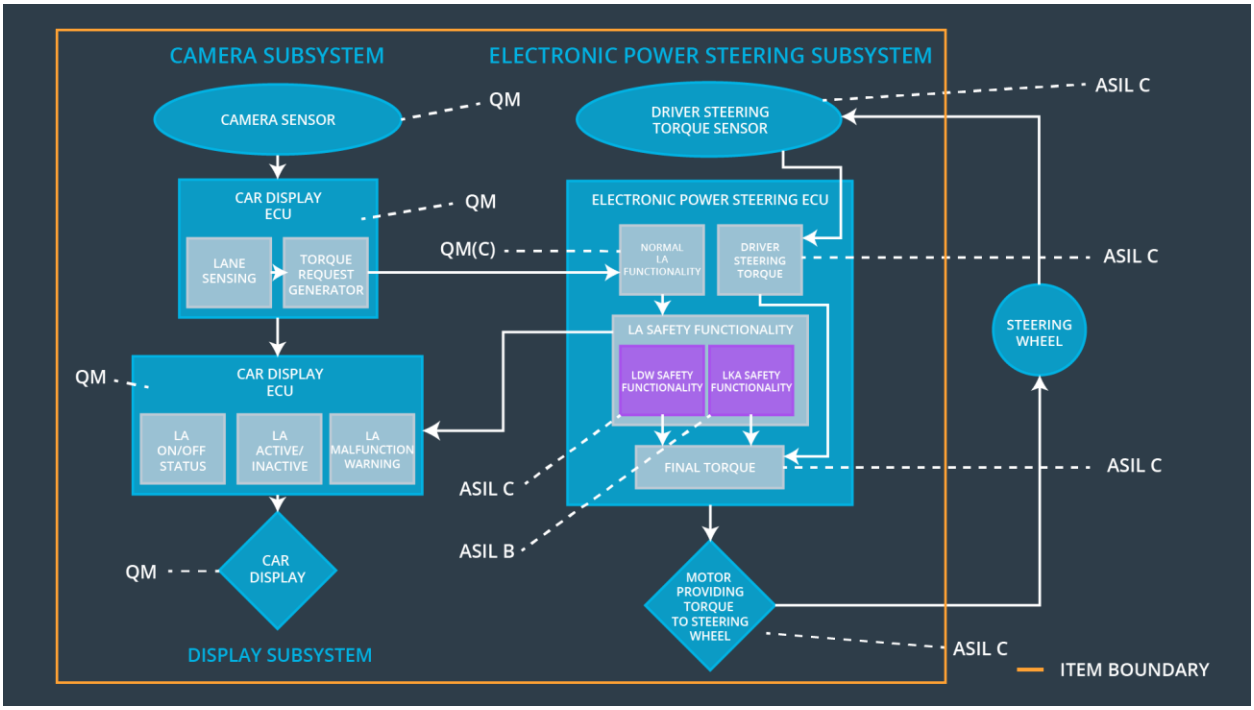
- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture As a subsequent step technical safety requirements will be considered within software and hardware implementation.

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	50 ms	LDW function is not activated
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Frequency	C	50 ms	LDW function is not activated
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied only for Max_Duration	B	500 ms	LKA function is not activated

Refined System Architecture from Functional Safety Concept

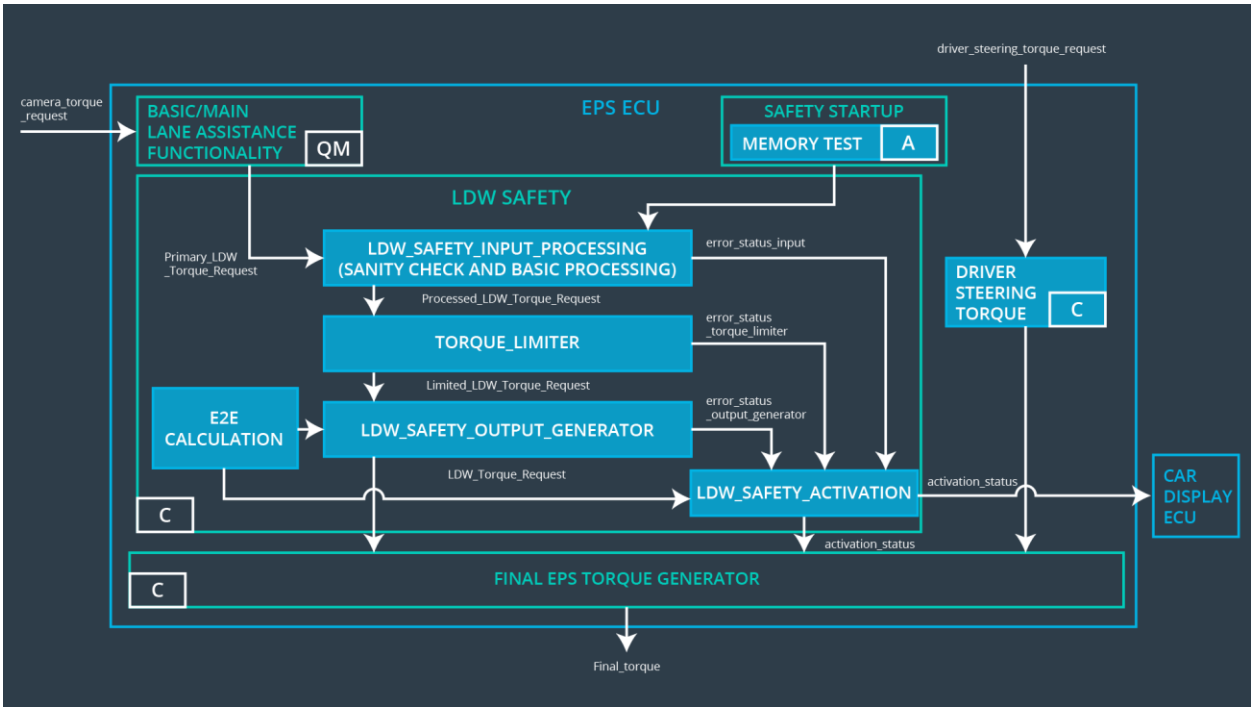


Functional overview of architecture elements

Element	Description
Camera Sensor	Provides images of road to camera sensor ECU.
Camera Sensor ECU - Lane Sensing	Detects the lane lines in camera images.
Camera Sensor ECU - Torque request generator	Generates an torque request to the Electronic Power Steering ECU.
Car Display	Shows warning to the driver.
Car Display ECU - Lane Assistance On/Off Status	Indicates if LKA is turned on.
Car Display ECU - Lane Assistant Active/Inactive	Indicates if LKA has properly detected lanes and is active at the moment.
Car Display ECU - Lane Assistance malfunction warning	Indicates malfunctioning of LKA.
Driver Steering Torque Sensor	Measures the torque applied by the driver on the

	steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Process input from Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	This module receives the torque request from Camera Sensor ECU.
EPS ECU - Lane Departure Warning Safety Functionality	Ensures torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures is LKA is not active for more than Max_Duration time.
EPS ECU - Final Torque	Combines the torque request from LKA and LDW functionalities and sends it to the Motor.
Motor	Applies the required 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 below Max_Torque_Amplitude	C	50ms	LDW Safety Block	The lane departure warning torque request amplitude shall be set to zero
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 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 warning light.	C	50ms	LDW Safety Block	
Technical	Memory test shall be conducted	A	Ignition	Separate	

Safety Requirement 05	at the startup of EPS ECU to check for any faults in memory.		cycle	External block with 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 Torque* component is below Max_Torque_Frequency	C	50ms	LDW Safety Component	The lane departure warning torque request amplitude shall be set to zero
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 to zero.	C	50ms	LDW Safety Component	
Technical Safety Requirement	As soon as the LDW function deactivates the LDW feature, the LDW safety software block shall	C	50ms	LDW Safety Component	

04	send a signal to the car display ECU to turn on a warning light.				
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	

Lane Keeping Assistance (LKA) Requirements:

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

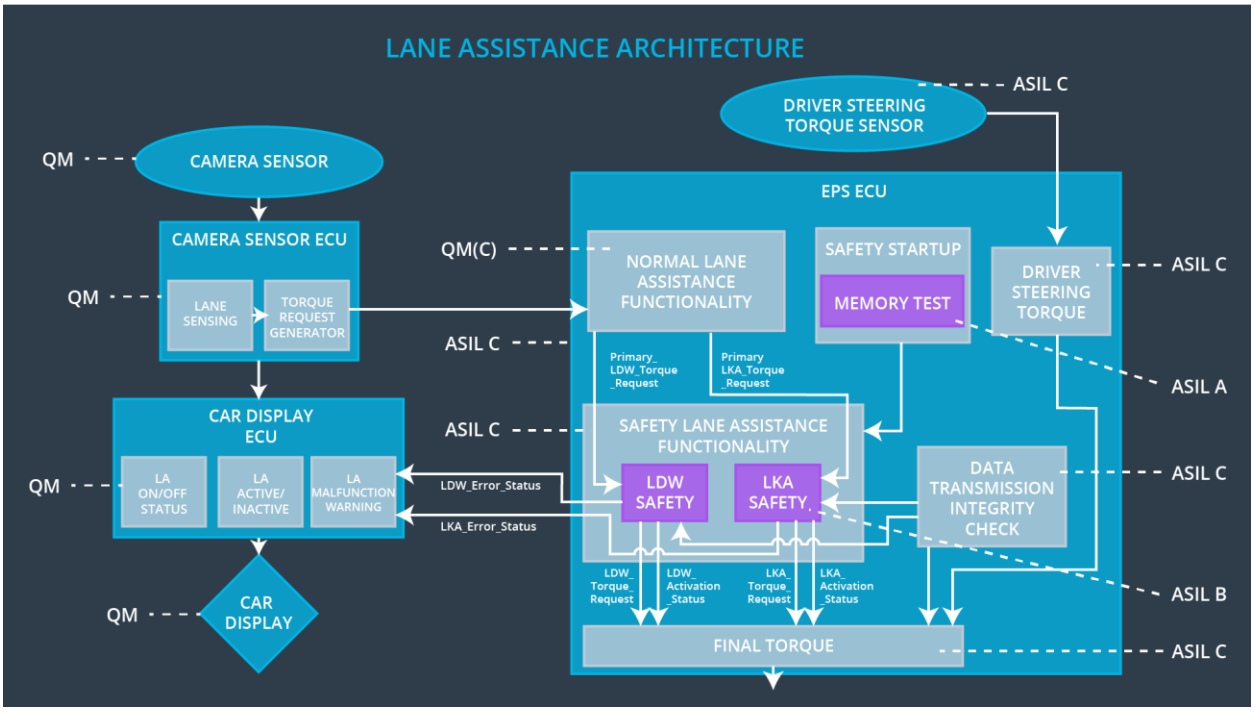
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 Requirement 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 Max_Torque_Duration	B	500ms	LKA safety component	The lane departure warning torque request
Technical Safety Requirement 02	Validity and Integrity of the data transmission for the LKA_Torque_Request signal shall be ensured	B	500ms	Data Transmission Integrity Check	
Technical Safety Requireme	As soon as a failure is detected by the LKA function, it shall	B	500ms	LKA safety component	

nt 03	deactivate the LKA feature and the LKA_Torque_Request shall be set to zero.				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

For 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