Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 2.0
Released on 2019-06-01

Document history

Date	Version	Editor	Description
01.06.2019	1.0	Sandeep Patil	Initial Version
02.06.2019	2.0	Sandeep Patil	Final Version

Table of Contents

Purpose of the Technical Safety Concept

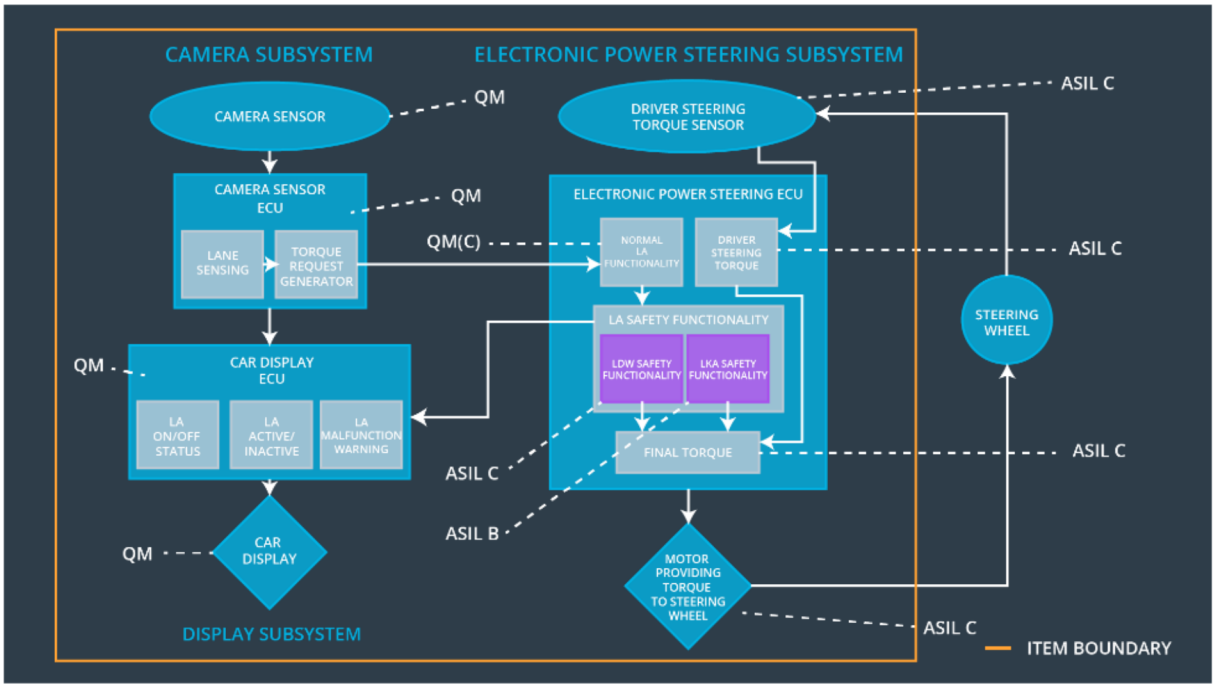
The purpose of this document is to derive new requirements that are more concrete and detail in item's technology as per ISO 26262

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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below MAX_TORQUE_AMPLITUDE	c	50 ms	Vibration torque amplitude < MAX_TORQUE_AMPLITUDE
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below MAX_TORQUE_FREQUENCY	c	50 ms	Vibration torque frequency < MAX_TORQUE_FREQUENCY
Functional Safety Requirement 02-01	The EPS Subsystem shall ensure that the LKA torque is applied only for MAX_DURATION	c	500 ms	LKA torque = 0

Refined System Architecture from Functional Safety Concept

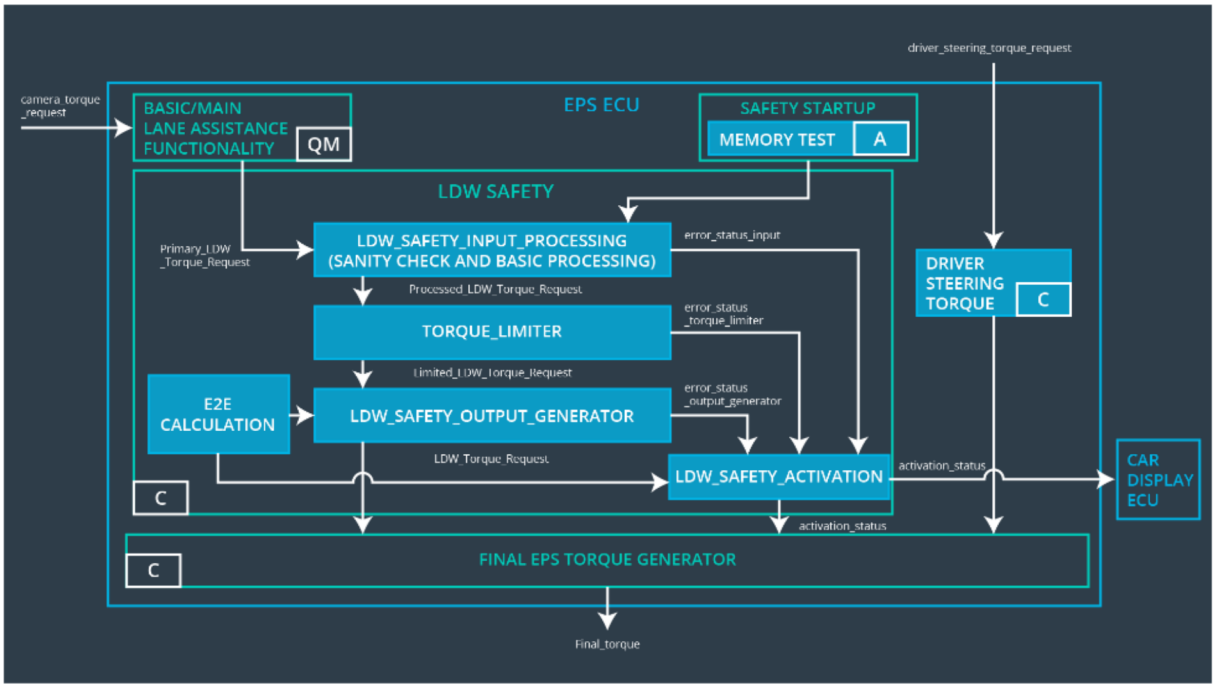


Functional overview of architecture elements

Element	Description
Camera Sensor	Capture image of the road and provide it to Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Detect lane lines and their position from the sensor
Camera Sensor ECU - Torque request generator	Calculate and request necessary torque to keep the ego vehicle in the lane
Car Display	Provide feedback to the driver regarding LAS Function enable status and LDW/LKS activation status
Car Display ECU - Lane Assistance On/Off Status	Drive the car display to show the function status information
Car Display ECU - Lane Assistant Active/Inactive	Drive the car display to show the function activation information

Car Display ECU - Lane Assistance malfunction warning	Drive the car display to show the function malfunction information
Driver Steering Torque Sensor	Measure the torque applied on steering wheel by driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receive torque applied by the driver
EPS ECU - Normal Lane Assistance Functionality	Receive requested torque from the Lane assist functionality
EPS ECU - Lane Departure Warning Safety Functionality	Module ensuring both torque amplitude and frequency is in the specified range
EPS ECU - Lane Keeping Assistant Safety Functionality	Module ensuring the LKA functionality is not activated more than specified time
EPS ECU - Final Torque	Calculate final effective torque from driver and LKS function and provide it to the motor
Motor	Apply the final torque calculated by the Electronic Power Steering ECU

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	The 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	50 ms	LDW Safety	LDW Torque = 0
Technical Safety Requirement 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	50 ms	LDW Safety	LDW Torque = 0
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	50 ms	LDW Safety	LDW Torque = 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	LDW Safety	LDW Torque = 0
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	ignition cycle	Data transmission and integrity check	LDW Torque = 0

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	The 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	50 ms	LDW Safety	LDW Torque = 0
Technical Safety Requirement 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	50 ms	LDW Safety	LDW Torque = 0
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	50 ms	LDW Safety	LDW Torque = 0

Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	LDW Safety	LDW Torque = 0
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	C	ignition cycle	Data transmission and integrity check	LDW Torque = 0

Lane Keeping Assistance (LKA) Requirements:

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

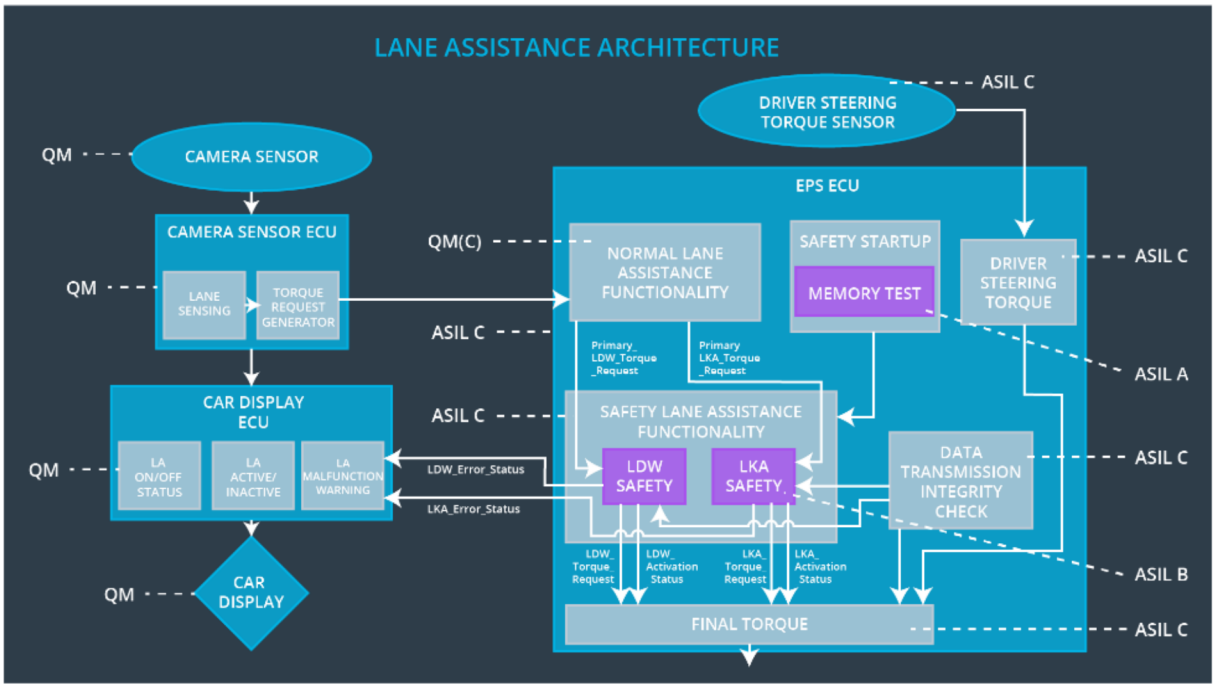
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 the duration of torque applied is applied for less than MAX_DURATION	C	500 ms	LKA Safety	LKA torque = 0
Technical Safety Requirement 02	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.	C	500 ms	LKA Safety	LKA torque = 0
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.	C	500 ms	LKA Safety	LKA torque = 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500 ms	LKA Safety	LKA torque = 0
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Data Transmission Integrity Check	LKA torque = 0

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	Technical Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	The 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.	**x**		
Technical Safety Requirement 01-01-02	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.	**x**		

Technical Safety Requirement 01-01-03	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.	**x**		
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	**x**		
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	**x**		
Technical Safety Requirement 01-02-01	The 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.	**x**		
Technical Safety Requirement 02-01-01	LKA safety component shall ensure the duration of torque applied is applied for less than MAX_DURATION	**x**		
Technical Safety Requirement 02-01-02	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.	**x**		

Technical Safety Requirement 02-01-03	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.	**x**		
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW functionality	Malfunction_01 Malfunction_02	Yes	LDW Malfunction warning on display
WDC-02	Turn off LKS functionality	Malfunction_03	Yes	LKS Malfunction warning on display