Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 2.1
Released on 2017-10-23

Document history

Date	Version	Editor	Description
Sep 12, 2017	1.0	Sampath Vanimisetti	Initial draft.
Sep 14, 2017	2.0	Sampath Vanimisetti	Added detail in software requirements section.
Oct 23, 2017	2.1	Sampath Vanimisetti	Minor corrections based on Review #794187

Table of Contents

Contents

Purpose of the Technical Safety Concept

The ISO 26262 standard emphasizes that functional safety concept should be used during the concept stage, whereas technical safety concept should be used during the product development stage. The technical safety concept is more concrete and gets into the details of the item's technology, hardware and software. In the item's product development phase, the technical safety concept aims to address development at two levels: (1) system level and (2) hardware and software level. Therefore, technical safety concept first translates function safety requirements to technical safety requirements and then allocates them to the system architecture elements. The steps taken to develop technical safety requirements from functional safety requirements based on the item definition are shown in Figure 1. The technical safety document can be divided in multiple sub-sections as shown in the following Figure 2.

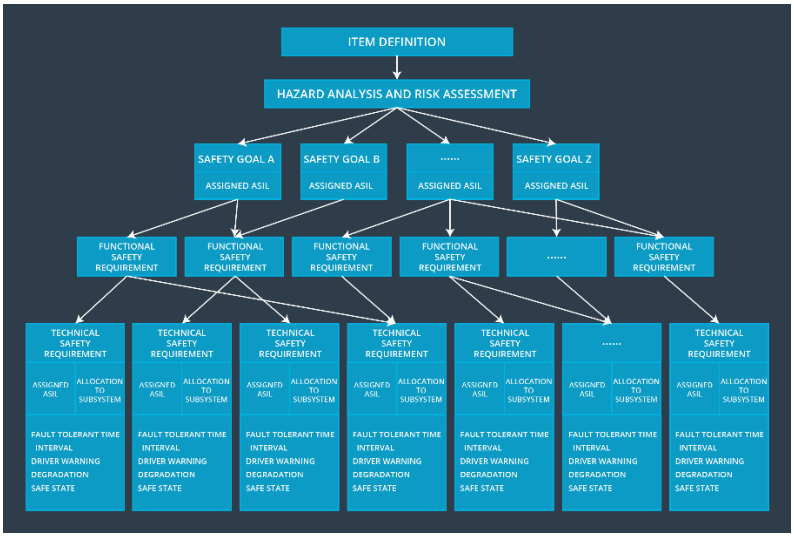

Figure 1: Steps taken in the developing the technical safety requirements from functional safety requirements.

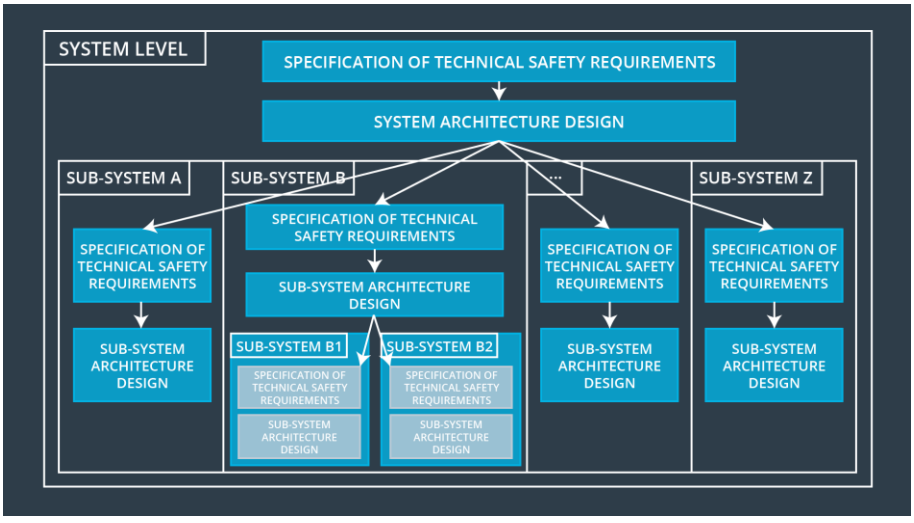

Figure 2: Overview of organization of the technical safety requirements document.

The technical safety requirements describe the signal flow in the system architecture and define which components are responsible for functionality associate with the signal flow. In the following sections, the technical safety requirements will be derived from the functional safety requirements and then allocated to individual hardware/software elements in the system architecture diagram. A quick overview of the functional safety requirements and the refined architecture diagram are shown before.

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	LDW shall ensure that steering oscillating torque amplitude is below MAX_StrOscTrqAmp	C	50 ms	Set steering oscillation torque amplitude to zero
Functional Safety Requirement 01-02	LDW shall ensure that steering oscillating torque amplitude is below MAX_StrOscTrqFrq	C	50 ms	Set steering oscillating frequency to zero
Functional Safety Requirement 02-01	LKA steering torque applied for less then duration MAX_LKAStrTrqDuration	B	500 ms	Set LKA torque value to 0
Functional Safety Requirement 02-02	LKA steering torque is set to zero upon malfunction of camera or when camera stops detecting lane markings on road	B	500 ms	Set LKA torque value to 0

Overview of the Refined of the System Architecture

The following Figure 3 shows the refined system architecture.

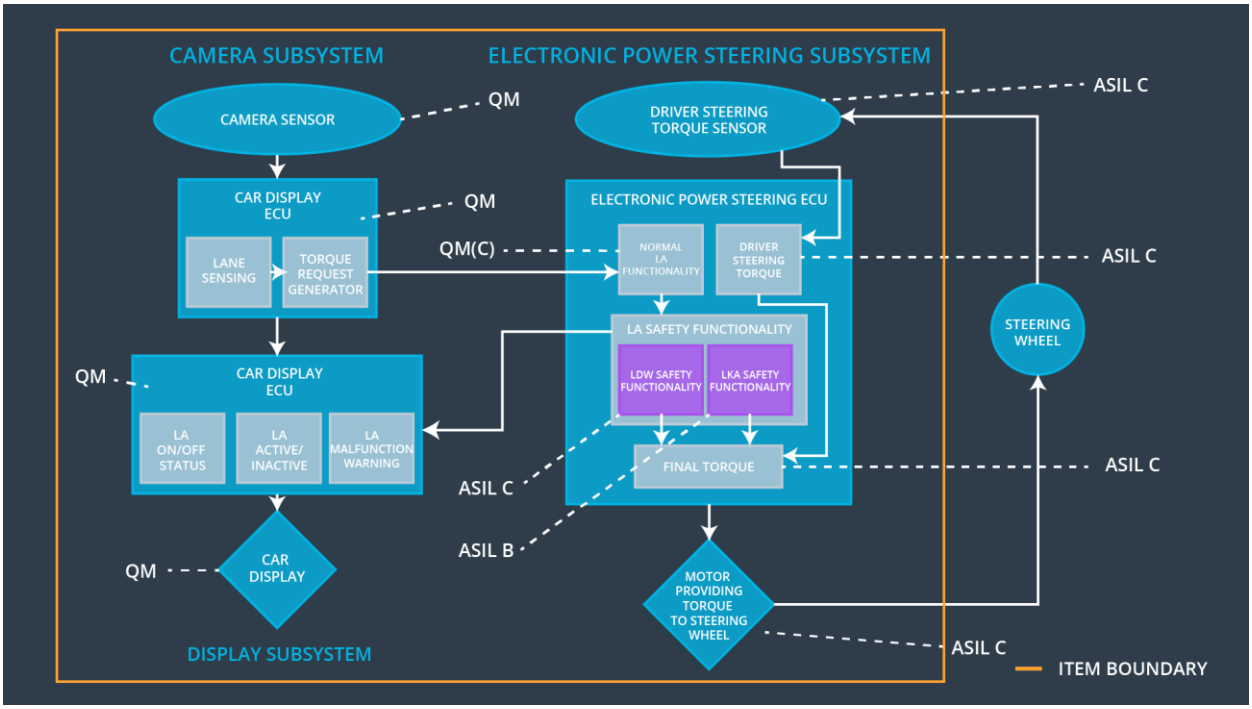

Figure 3: Overview of refined system architecture of lane assistance item.

Description of architecture elements for the refined system architecture.

Element	Description
Camera Sensor	Sense or capture the view of the road in front of the vehicle. The camera sensor outputs the raw video frame feed to the camera sensor ECU.
Camera Sensor ECU – Lane Sensing	Process the raw video frame feed provided by the camera sensor and identify regions-of-interest (ROIs) from each image frame. This will include identification of the lane marking on the road.
Camera Sensor ECU – Torque Request Generator	The ECU will determine the current position of vehicle in the ego-lane, distance to each lane marking and the curvature of the road ahead of the vehicle.
Car Display	Provide status and feedback for lane assistance items to the driver. For example, activation and deactivation of LDW/LKA, LDW alerts, etc.

Car Display ECU – LKA on/off status	Send signal to car display indicating LKA/LDW ON/OFF status.
Car Display ECU – LKA active/inactive status	Send signal to car display indicating LKA/LDW active/inactive status.
Car Display ECU – malfunction warning indication	Send signal to car display indicating LKA/LDW malfunction.
Driver Steering Torque Sensor	Sense the torque being applied by the driver on the steering wheel. Also, encode and transmit the current steering angle back to steering control ECU.
Electronic Power Steering ECU	Software module in EPS ECU that receives data from steering torque sensor (driver input) and steering angle sensor.
Electronic Power Steering ECU – Normal LA functionality	Software module in EPS ECU that receives data from the camera sensor ECU to determine how much steering torque to apply to steering wheel.
Electronic Power Steering ECU – LDW safety functionality	Software module in EPS ECU responsible for keeping the LDW oscillating torque amplitude and frequency below maximum prescribed values.
Electronic Power Steering ECU – LKA safety functionality	Software Module in EPS ECU responsible for limiting the LKA steering torque application duration to no more than the maximum prescribed value.
Electronic Power Steering ECU – final torque output	Software module EPS ECU responsible to receive request from LDW and LKA software modules and limit the final torque output request to below the maximum prescribed value.
Final Torque Motor	Receive commands from electronic power steering ECU and apply required torque amplitude and frequency for prescribed duration.

Technical Safety Concept

Functional Safety Requirements for LDW:

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	Lane Assist item shall ensure that the LDW oscillating steering torque amplitude is below the MAX_StrOscTrqAmp.	**x**		
Functional Safety Requirement 01-02	Lane Assist item shall ensure that the LDW oscillating steering torque frequency is below the MAX_StrOscTrqFrq..	**x**		

Technical Safety Requirements for LDW (see Figure 4 for allocation):

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01-a	Power-on memory status check to be performed by EPS ECU	A	Acc Key on Cycle	Safety Startup Memory Test Block	Disable LDW and set malfunction on display.
Technical Safety Requirement 01-b	Check validity and integrity of the of data transmission for ‘LDW_TrqReq’ signal .	C	50 ms	Data transmission integtrity check block	Set LDW torque amp & freq to zero and set malfunction on display.
Technical Safety Requirement 01-c	The LDW safety block shall ensure that amp & freq of ‘LDW_TrqReq' sent to EPS ECU is below MAX_StrOscTrqAmp and MAX_StrOscTrqFrq	C	50 ms	LDW Safety Block	Set LDW torque amp & freq to zero.

Technical Safety Requirement 01-d	When failure is detected, disable LDW, set LDW_TrqReq to 0 and send signal to display ECU to turn on the LDW warning light	C	50 ms	LDW Safety	LDW torque output is set to zero

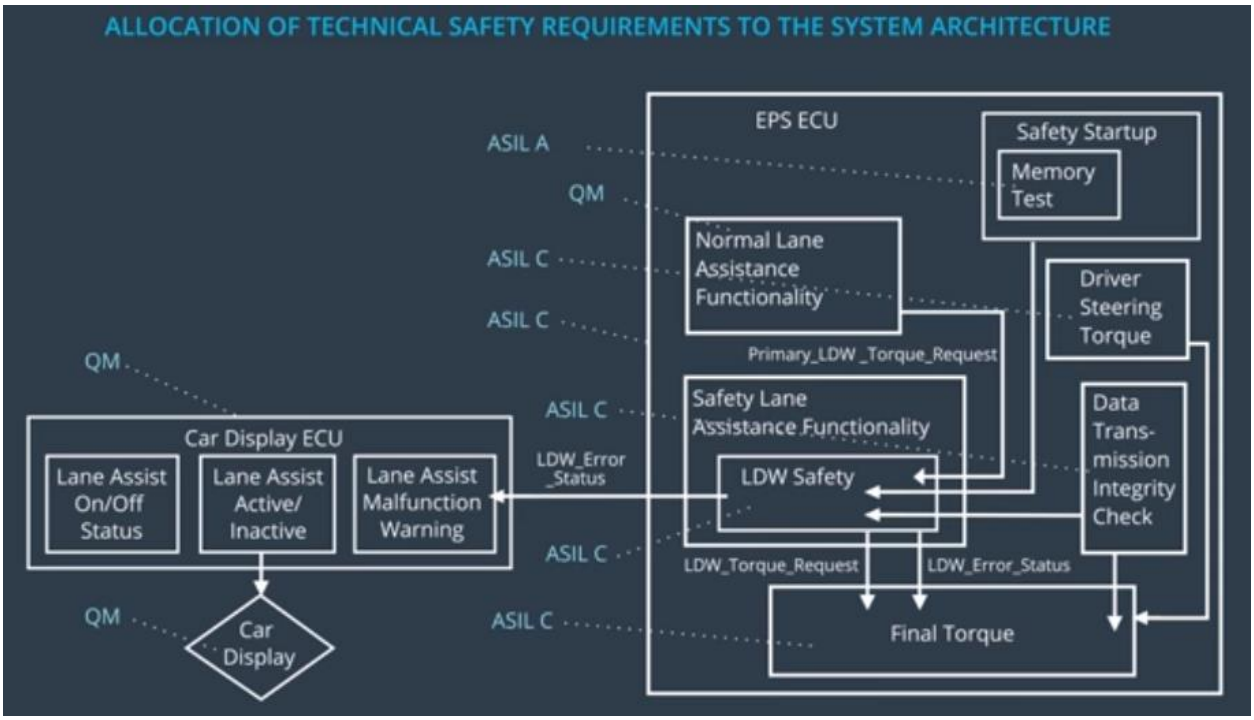

Figure 4: Allocation of requirement to system architecture for LDW item.

LDW Verification & Validation Criteria:

ID	Verification Acceptance Criteria and Method	Validation Acceptance Criteria and Method
Technical Safety Requirement 01-a	Verify using intentional memory fault to see if the software is identifying fault.	Validate using HIL simulation that the software is disabling the LDW function as soon as it detects the memory fault and sets LDW_Error_Status.
Technical Safety Requirement 01-b	Verify that the Data Transmission Integrity Check is receiving data with the CRC check. .	Compare and validate the CRC checks with the data transmitted between LDW safety module and final torque module in ECU software. Validate if display is set or now.
Technical Safety	Verify that the LDW_Torque_Request and LDW_Erro_Status are being set if	Validate using HIL simulation to see if the torque amplitude and frequency is

Requirement 01-c	amp & freq are above MAX_StrOscTrqAmp and MAX_StrOscTrqFrq	being set to zero.
Technical Safety Requirement 01-d	Verify that when failure is detected, LDW is disabled, LDW_TrqReq is 0 and display warning light is on	For HIL simulated failure, validate LDW is disabled, torque request is set to 0 and display warning light is on.

Functional Safety Requirements for LKA:

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	EPS ECU will ensure that the LKA steering torque is applied for no more than MAX_LKAStrTrqDuration	**x**		
Functional Safety Requirement 02-02	EPS ECU will ensure that LKA steering torque is set ot zero if camera malfunctions or lane marking are not visible	**x**		

Technical Safety Requirements for LKA (see Figure 5 for allocation):

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 02-a	LKA component to ensure that duration of torque assist is less is less than MAX_LKAStrTrqDuration	B	500 ms	LKA Safety Block	Set LKA torque to zero
Technical Safety Requirement 02-b	Power-on memory status check to be performed by EPS ECU	A	Acc Key on Cycle	Safety Startup Memory Test Block	Disable LKA and set malfunction on display.

Technical Safety Requirement 02-c	Check validity and integrity of the of data transmission for 'LKA_TrqReq' signal .	B	500 ms	Data transmission integtrity check block	Set LKA torque to zero
Technical Safety Requirement 02-d	LKA item shall ensure that LKA_Torque_Request is set to zero if road or lanes are not visible	B	500 ms	LKA Safety Block	Set LKA torque to zero
Technical Safety Requirement 02-e	When failure is detected, disable LKA, set LKA_Torque_Request to 0 and send signal to display ECU to turn on the LKA warning light	B	500 ms	LKA Safety Block	Set LKA torque to zero

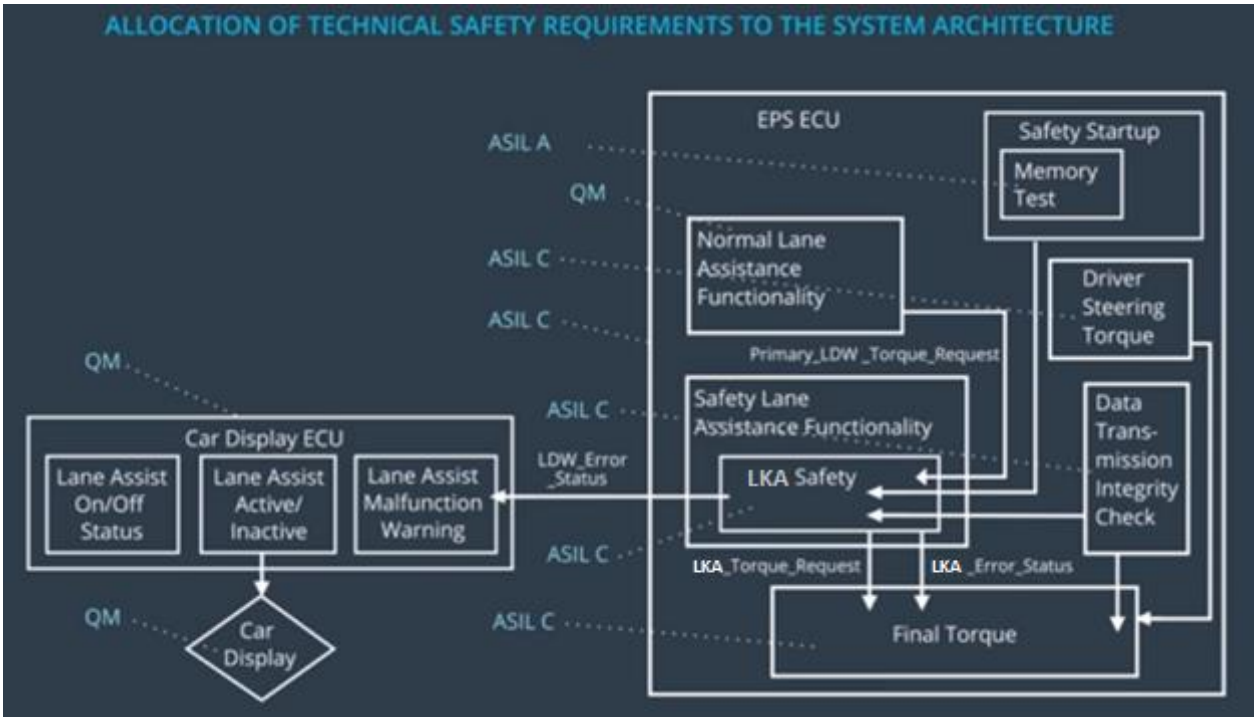

Figure 5: Allocation of requirement to system architecture for LKA item.

LKA Verification & Validation Criteria:

ID	Verification Acceptance Criteria and Method	Validation Acceptance Criteria and Method
Technical Safety Requirement 02-a	Verify using intentional memory fault to see if the software is identifying fault.	Validate using HIL simulation that the software is disabling the LDW function as soon as it detects the memory fault and sets LKA_Error_Status.
Technical Safety Requirement 02-b	Verify that the Data Transmission Integrity Check is receiving data with the CRC check.	Compare and validate CRC checks with data transmitted between LKA safety module & final torque module. Validate if display is set or no.
Technical Safety Requirement 02-d	Verfiy that LKA_Torque_Request is set to zero if road or lanes are not visible	Validate using HIL simulation to see if torque is assigned for only a short duration defined by MAX_LKAStrTrqDuration.
Technical Safety Requirement 02-e	Verify that when failure is detected, LKA is disabled, LKA_TrqReq is 0 and display warning light is on.	For HIL simulated failure, validate LKA is disabled, torque request is set to 0 and display warning light is on.

Refined System Architecture after Technical Safety Concept

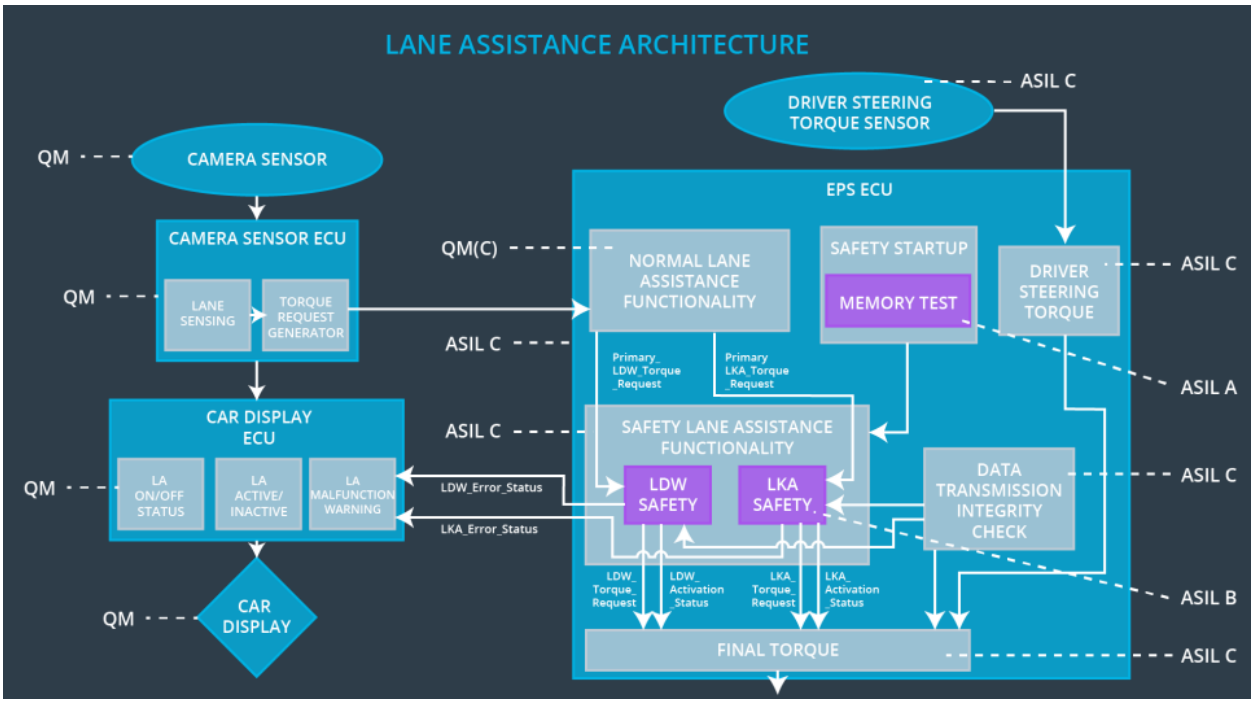

Figure 6: Refinement and allocation of technical requirements to lane assistance architecture.

Functional overview of architecture elements

Element	Description
Camera Sensor	Capture video frames of road in front of the vehicle and transmit data to camera ECU.
Camera Sensor ECU - Lane Sensing	Software block in camera ECU responsible for detecting the lane lines and identifying position of the vehicle in the ego-lane.
Camera Sensor ECU - Torque request generator	Software block in camera ECU responsible for calculating the torque required based input data from the lane sensing module.
Car Display	Display software block is responsible for displaying the status, warnings and malfunction indications related to LDW/LKA.
Car Display ECU - Lane Assistance On/Off Status	Software block in car display ECU that show status of LDW/LKA.
Car Display ECU - Lane Assistant Active/Inactive	Software block in car display ECU that show if LDW/LKA are active or inactive.
Car Display ECU - Lane Assistance malfunction warning	Software block in car display ECU that show if LDW/LKA have malfunctioned.
Driver Steering Torque Sensor	Sensor that measure the steering torque and current angle applied by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software block in EPS ECU that receives the torque request generated by the camera sensor ECU and converts into signals for steering motor.
EPS ECU - Normal Lane Assistance Functionality	Software block in EPS ECU that receives the torque request generated by the camera sensor ECU and converts into signals for steering motor to perform the LDW or LKA functions normally.
EPS ECU - Lane Departure Warning Safety Functionality	Software block in EPS ECU that receives lane departure condition from camera ECU and then sends appropriate steering oscillation amplitude and frequency to steering motor.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software block in EPS ECU that receives lane curvature from camera ECU and then sends appropriate steering torque for specified duration to the steering motor.

EPS ECU - Final Torque	Software block in EPS ECU that combines LDW or LKA torque requests and sends it to motor.
EPS ECU - Startup Memory Test Check	Software block in EPS ECU that perform startup safety checks to ensure that there are no memory faults.
EPS ECU - Data Transmission Integrity Check	Software block that checks the integrity of transmitted data using CRC checks or similar.
Steering motor	Actuator that applied requested steering torque amplitude and frequency for specified duration by the EPS ECU.

Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are assigned to EPS software block in ECU. See below table.

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	Lane Assist item shall ensure that the LDW oscillating steering torque amplitude is below the MAX_StrOscTrqAmp.	**x**		
Functional Safety Requirement 01-02	Lane Assist item shall ensure that the LDW oscillating steering torque frequency is below the MAX_StrOscTrqFrq..	**x**		
Functional Safety Requirement 02-01	EPS ECU will ensure that the LKA steering torque is applied for no more than MAX_LKAStrTrqDuration	**x**		
Functional Safety Requirement 02-01	EPS ECU will ensure that LKA steering torque is set ot zero if camera malfunctions or lane marking are not visible	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW	Malfunction_01 to Malfunction_04	LDW steering osc torque amp & frq set to 0	Set LDW malfunction on car display ECU
WDC-02	Turn off LKA	Malfunction_05, Malfunction_06	LKA steering torque set to 0	Set LKA malfunction on car display ECU