Elektrobit

UDACITY

Software Safety Requirements and Architecture

Lane Assistance

Document Version:1.0

Document history

Date	Version	Editor	Description
27/11/2018	1.0	Atul Kumar	Draft version
29/11/2018	2.0	Atul Kumar	Adding more feature

Table of Contents

Purpose

The purpose of the software safety requirements and architecture document is to identify new detailed requirements and allocate these software requirements to component level diagrams for the lane assistance functional safety project as pertain to the potential malfunctions of the electrical and electronic systems as defined by ISO 26262 standard or tailored version as per organization.

Inputs to the Software Requirements and Architecture Document

Technical safety requirements

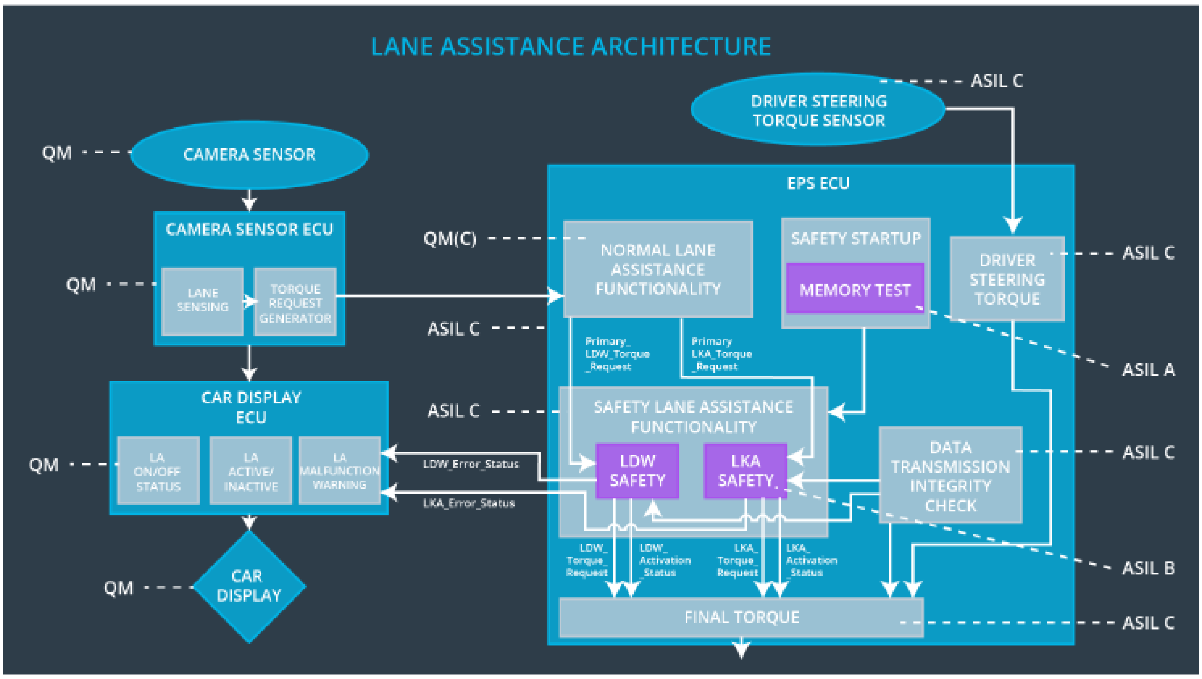
Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety 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	50ms	LDW Safety block	Set lane departure warning torque to zero
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	50ms	LDW Safety block	Set lane departure warning torque 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	Set lane departure warning torque to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	A	50ms	LDW Safety block	Set lane departure warning torque to zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Data Transmission Integrity Check	Set lane departure warning torque to zero

Technical Safety Requirement 06	The LDW safety component shall ensure that the fequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Fequency	C	50ms	LDW Safety block	Set lane departure warning torque to zero
Technical Safety Requirement 07	The LKA safety component shall ensure that the duration of the lane keeping assistance torque applied is less than Max_Duration.	C	500ms	LKA Safety block	Set lane keeping assistance torque to zero
Technical Safety Requirement 08	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	500ms	LKA Safety block	Set lane keeping assistance torque to zero
Technical Safety Requirement 09	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	500ms	LKA Safety block	Set lane keeping assistance torque to zero
Technical Safety Requirement 10	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured	C	500ms	LKA Safety block	Set lane keeping assistance torque to zero
Technical Safety Requirement 11	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	Set lane keeping assistance torque to zero
Technical Safety Requirement 12	The LKA safety component shall ensure that the loss of camera sensor torque request transmission will deactivate the LKA feature and the	C	500ms	LKA Safety block	Set lane keeping assistance torque to zero

	'LKA_Torque_Request' shall be set to zero.				

Refined Architecture Diagram from the Technical Safety Concept



Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

[Instructions: Fill in the software safety requirements for the LDW amplitude malfunction technical safety requirements. We have provided the associated technical safety requirements. Hint: The software safety requirements were discussed in the text from the software and hardware lesson.

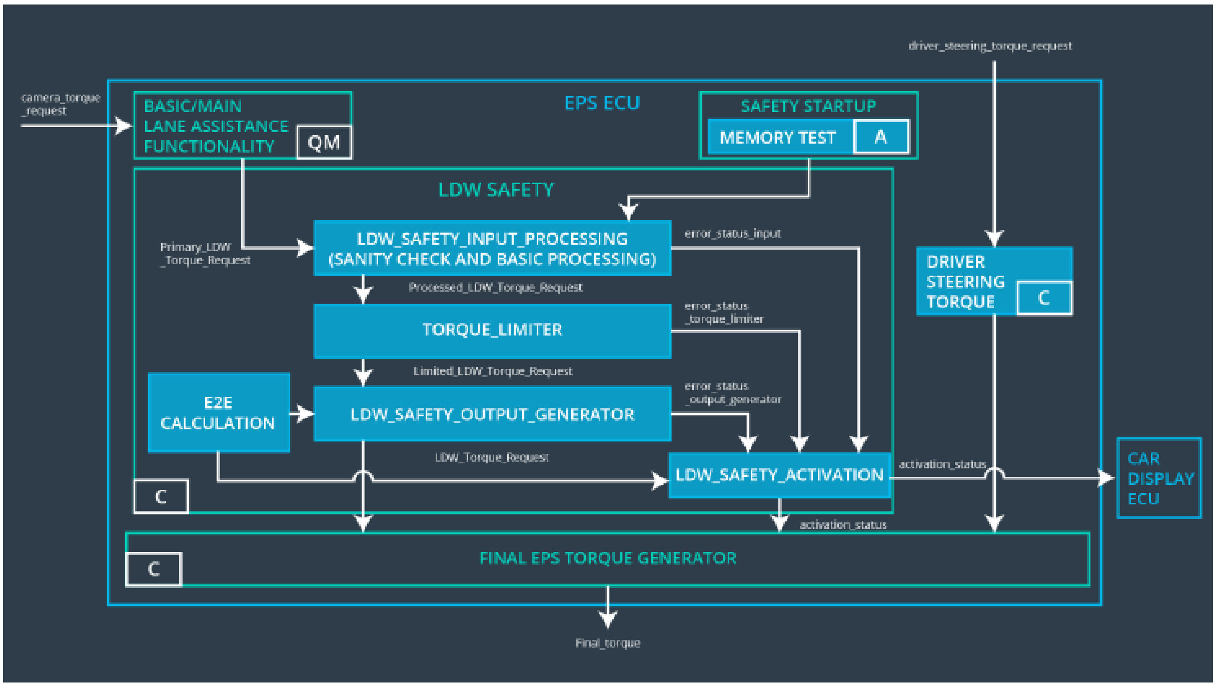
OPTIONAL:

CHALLENGE ONE
Develop software safety requirements for the Lane Departure Warning (LDW) frequency function and modify the system architecture as needed.

CHALLENGE TWO

Develop software safety requirements for the Lane Keeping Assistance (LKA) function and modify the system architecture as needed.
]

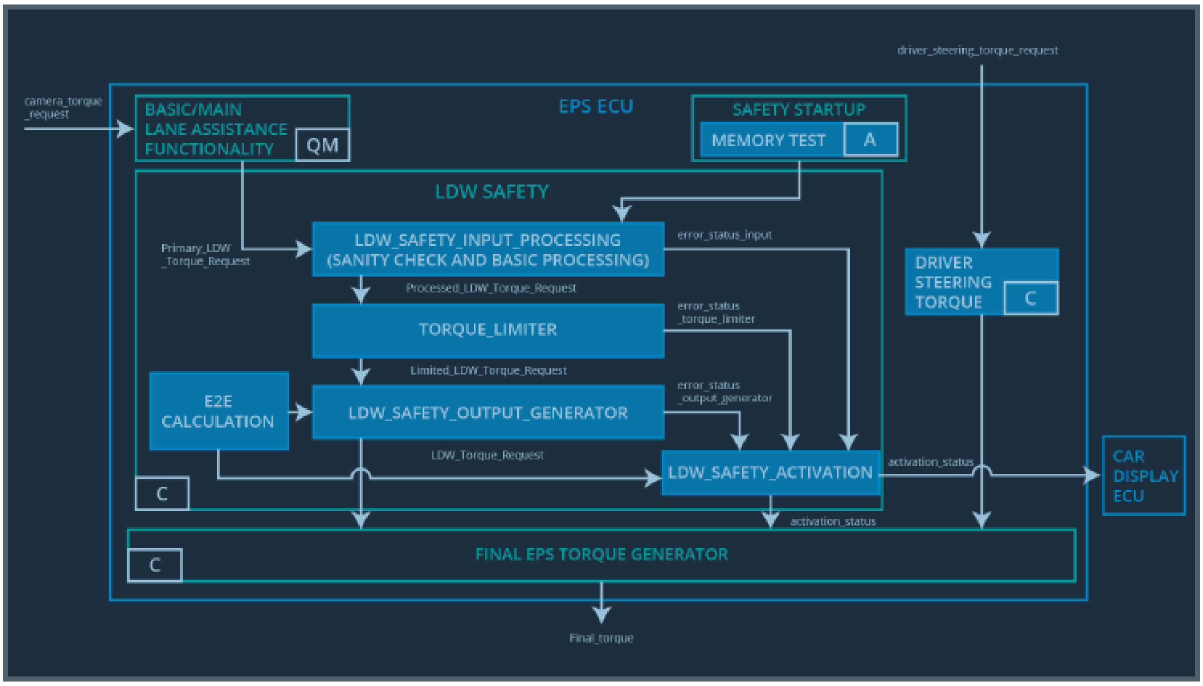
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the Final Electronic Power Steering Torque component is below Max_Torque_Amplitude	c	50ms	LDW Safety block	Set lane departure warning torque to zero


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
DRIVER STEERING TORQUE
C
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement	The input signal “Primary_LDW_Torq_Req” shall be read and pre-processed to	C	LDW_SAFETY_INPUT_PROCESSING	Not Applicable

01-01	determine the torque request coming from the “Basic/Main LAFunctionality” SW Component. Signal“processed_LDW_Torq_Req”shall be generated at the end of the processing			
Software Safety Requirement 01-02	In case the “processed_LDW_Torq_Req” signal has a value greater than“Max_Torque_Ampltide_LDW”(maximum allowed safe torque), the torque signal “limited_LDW_Torq_Req” shall be set to 0, else“limited_LDW_Torq_Req” shall take the value of “processed_LDW_Torq_Req”	C	TORQUE_LIMITER	“limited_LDW_Torq_Req” = 0(Nm=Newtonmeter)
Software Safety Requirement 01-03	The“limited_LDW_Torq_Req”shall be transformed into a signal “LDW_Torq_Req” which is suitable to be transmitted outside of the LDW Safety component (“LDW Safety”) to the “Final EPS Torque” component.	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

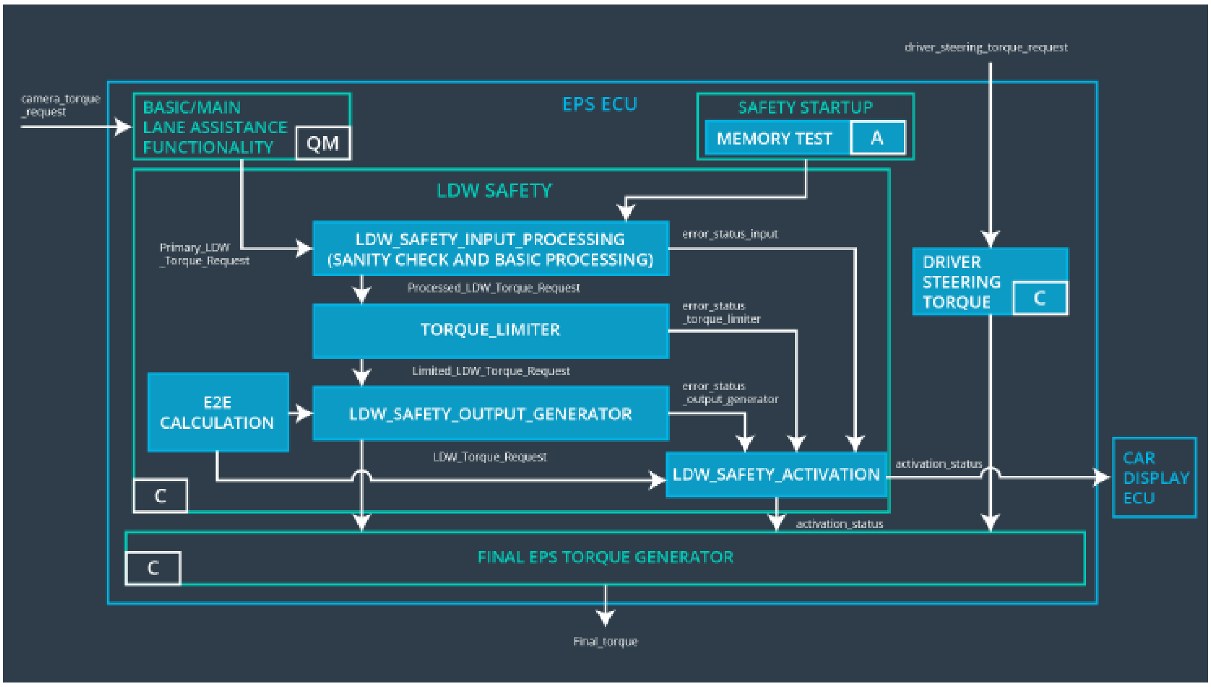
ID	Technical Safety Requirement	A S I L	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW_Torque_Request shall be set to zero	C	50ms	LDW Safety block	Set lane departure warning torque to zero


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 02-01	Each of the SW elements shall output a signal to indicate any error which is detected by the element. Error signal = error_status_input(LDW_SAFETY_INPUT_PROCESSING), error_status_torque_limiter(TOR	C	All	Not Applicable

	C All N/A 8 QUE_LIMITER), error_status_output_gen(LDW_SAFETY_OUTPUT_GENERATOR)			
Software Safety Requirement 02-02	A software element shall evaluate the error status of all the other software elements and in case any 1 of them indicates an error, it shall deactivate theLDW feature(“activation_status”=0)	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)
	In case of no errors from the software elements, the status of the LDW feature shall be set to activated (“activation_status”=1)		LDW_SAFETY_ACTIVATION	Not Applicable
	In case an error is detected by any of the software elements, it shall set the value of its corresponding torque to 0 so that “LDW_Torq_Req” is set to 0		ALL	LDW_Torq_Req= 0 (Nm)
	Once the LDW functionality has been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again.	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)

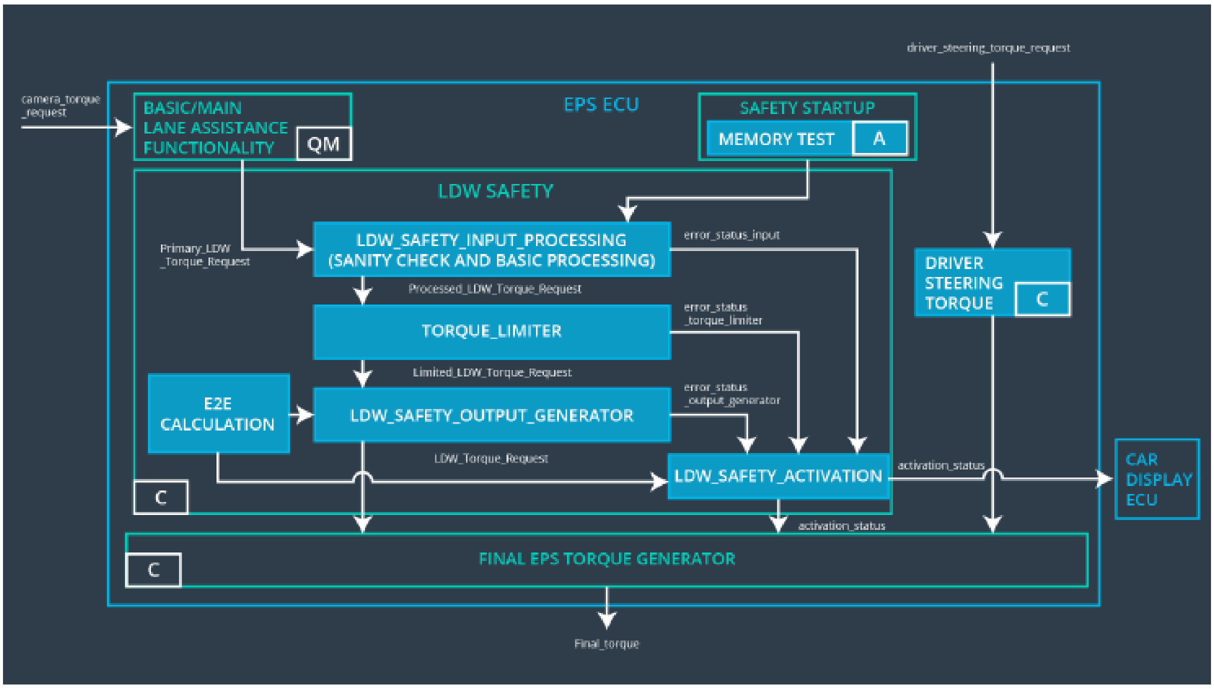
ID	Technical Safety Requirement	A S I L	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 03	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light	C	50ms	LDW Safety block	Set lane departure warning torque to zero


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	When the LDW function is deactivated (activation_status set to 0), the activation_status shall be sent to the car displayECU.	C	LDW_SAFETY_ACTIVATION, CarDisplay ECU	Not Applicable

	Technical Safety Requirement	A	Fault	Allocation to	Safe State

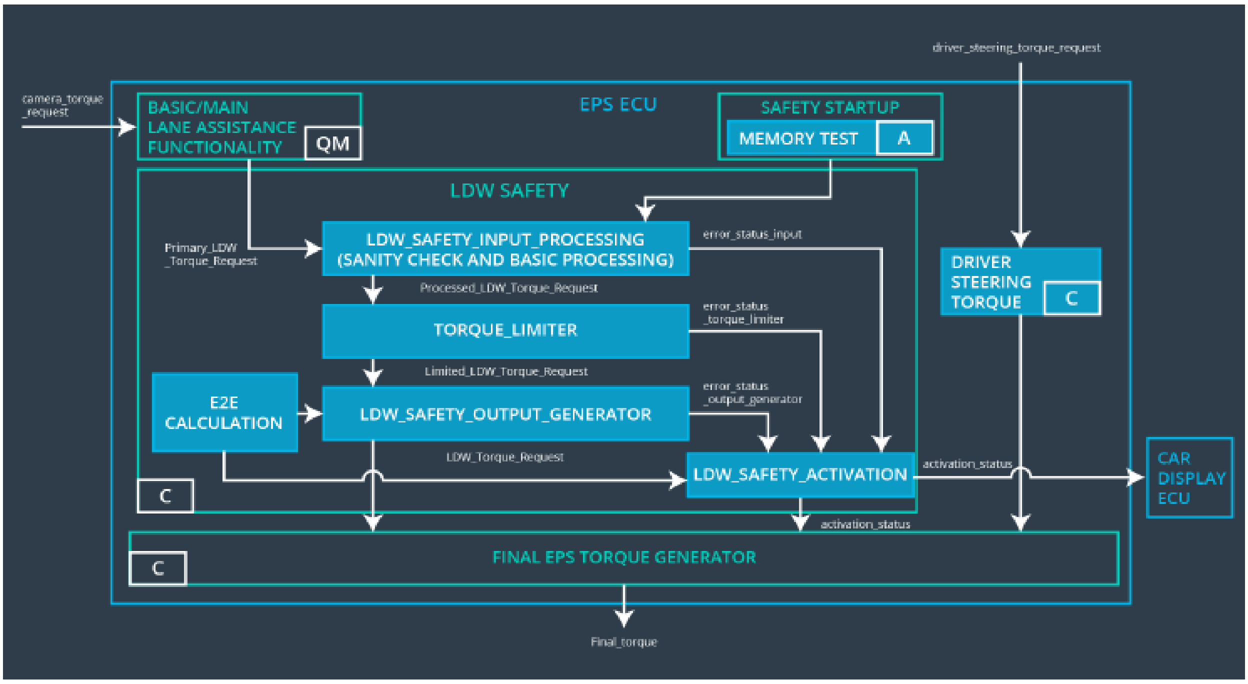
		S I L	Tolerant Time Interval	Architecture	
Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light	C	50ms	LDW Safety block	Set lane departure warning torque to zero


driver_steering_torque_request
camera_torque _request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
Primary_LDW _Torque_Request
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status _torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status _output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

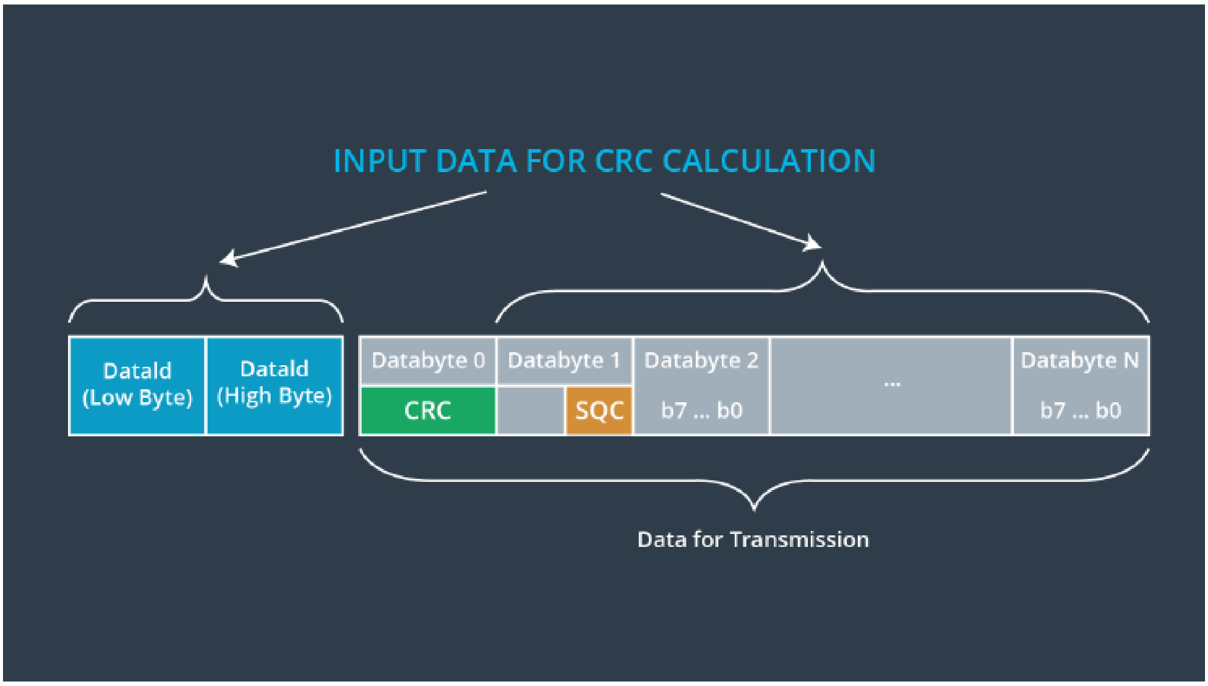
ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	When the LDW function is deactivated (activation_status set to 0), the activation_status shall be sent to the car displayECU	C	LDW_SAFETY_ACTIVATION,CarDisplay ECU	Not Applicable

ID	Technical Safety Requirement	A S I L	Fault Tolerant Time Interval	Allocation to Architecture	Safe State

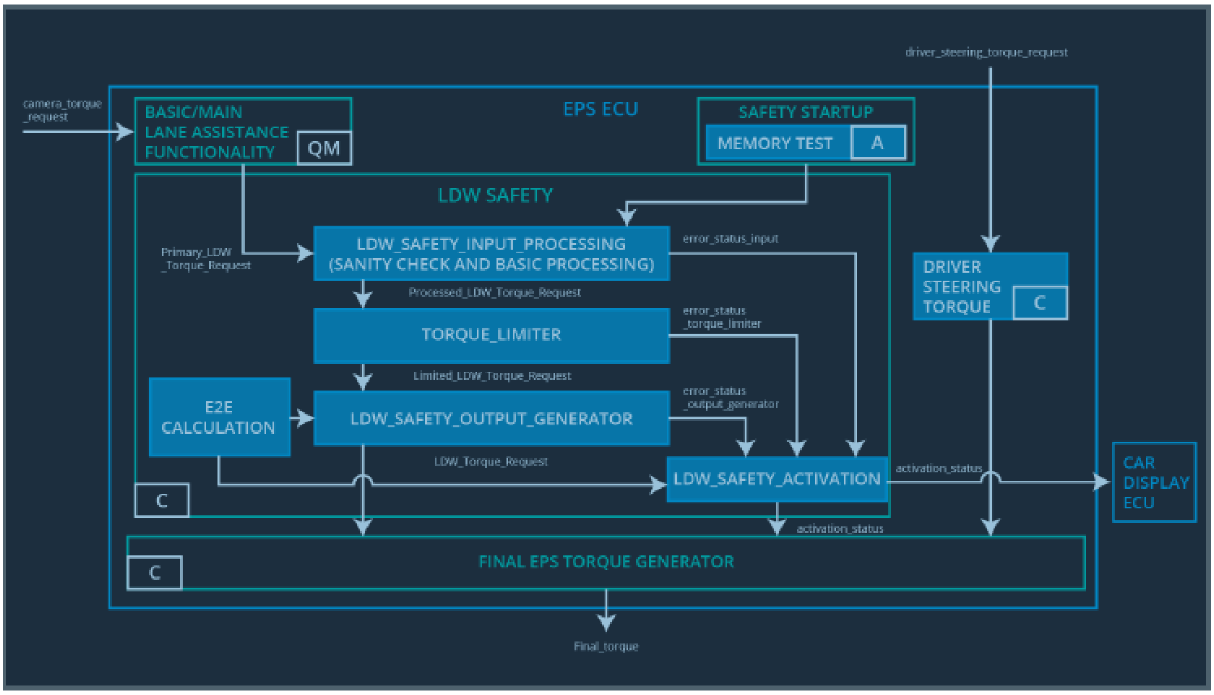
Technical Safety Requirement 04-01	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50ms	Data Transmission Integrity Check	Not Applicable


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	Any data to be transmitted outside of the LDW Safety component (“LDW Safety”)including "LDW_Torque_Req" and “activation_status” shall be protected by an End2End protection mechanism	C	E2ECalc	LDW_Torq_Req=0(Nm)
	The E2E protection protocol shall contain and attach the control data: alive counter (SQC) and CRC to the data to be transmitted.	C	E2ECalc	LDW_Torq_Req=0(Nm)



ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Data Transmission Integrity Check	Set lane departure warning torque to zero

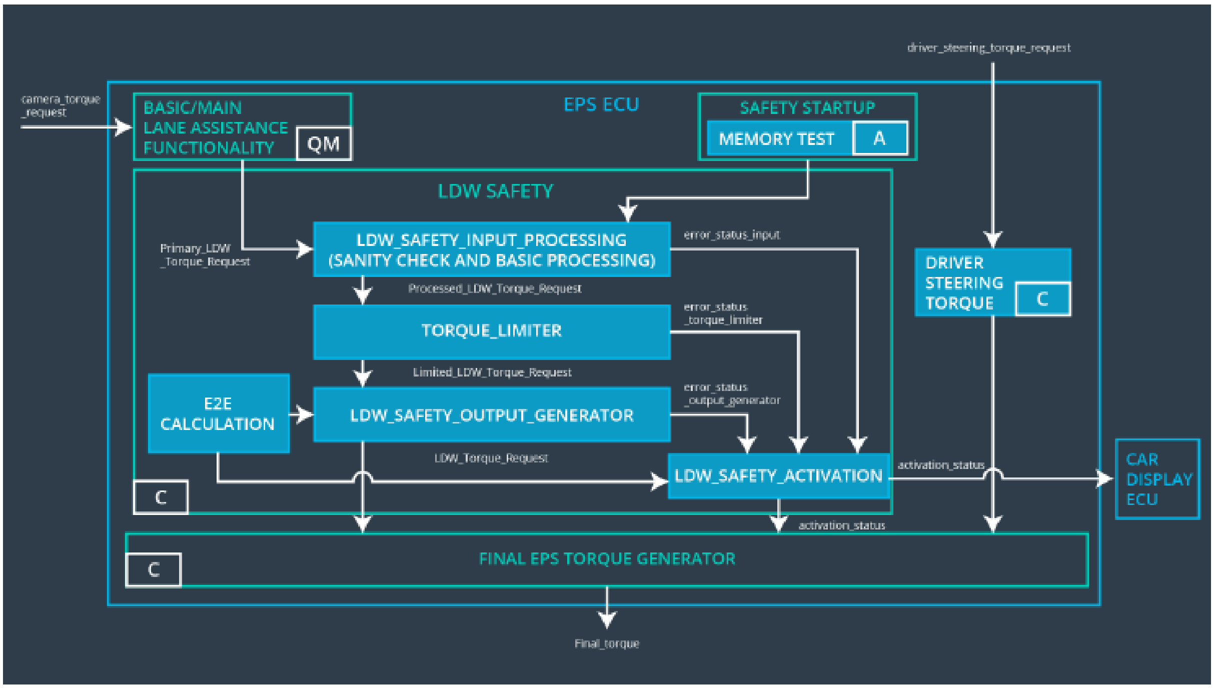

driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
C
DRIVER STEERING TORQUE
C
CAR DISPLAY ECU
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	A CRC verification check over the software code in the Flash memory shall be done every time the ignition is switched from off to on to check for any corruption of content.	A	MEMORYTEST	Activation_status=0
Software Safety Requirement 04-01	Standard RAM tests to check the data bus, address bus and device integrity shall be done every time the ignition is switched from off to on.	A	MEMORYTEST	Activation_status=0
Software Safety Requirement 04-01	The test result of the RAM or Flash memory shall be indicated to the LDW_Safety component via the “test_status” signal	A	MEMORYTEST	Activation_status=0
Software Safety Requirement 04-01	In case any fault is indicated via the “test_status” signal the INPUT_LDW_PROCESSING shall set an error on error_status_input (=1) so that	A	LDW_SAFETY_PROCESSING	Activation_status=0

	the LDW functionality is deactivated and the LDWTorque is set to 0			

Lane Departure Warning(LDW) Frequency Malfunction Software Requirements:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	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 block	Set lane departure warning torque to zero


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
DRIVER STEERING TORQUE
C
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

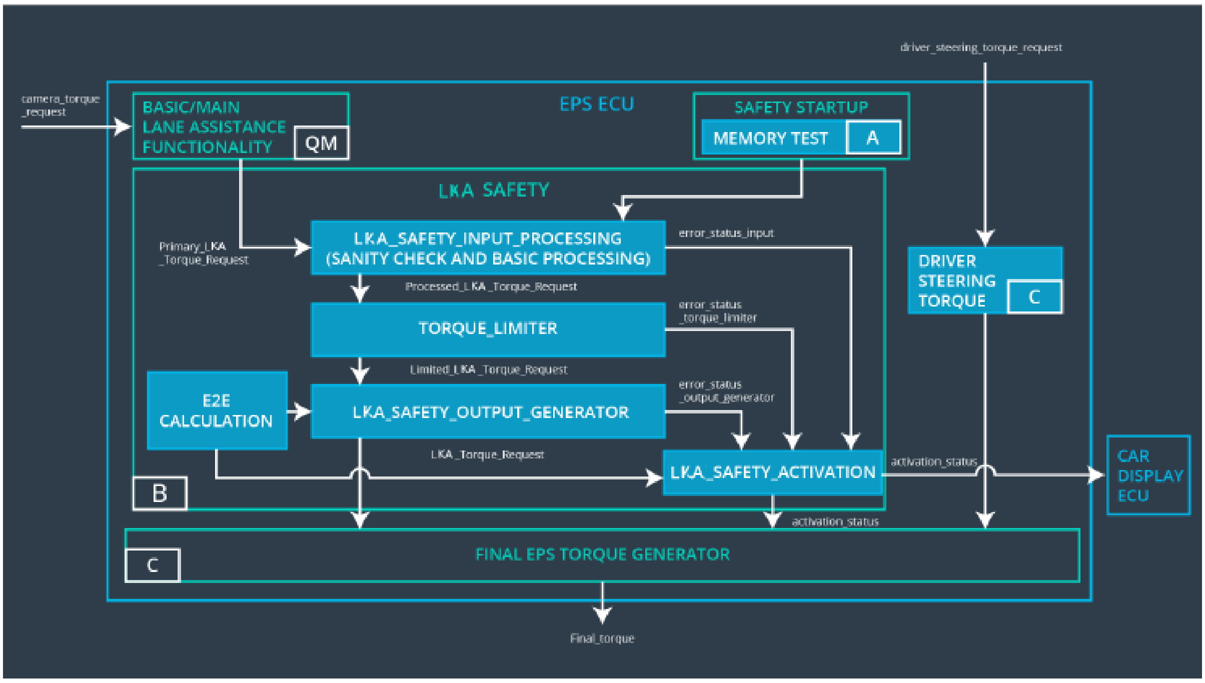
ID	Software Safety Requirement	ASI	Allocation Software Elements	Safe State

		L		
Software Safety Requirement 04-01	The input signal “Primary_LDW_Torq_Req” shall be read and pre-processed to determine the torque request coming from the “Basic/Main LA Functionality” SW Component. Signal“processed_LDW_Torq_Req”shall be generated at the end of the processing.	C	LDW_SAFETY_INPUT_PROCESSING	Not Applicable
Software Safety Requirement 04-02	In case the “processed_LDW_Torq_Req” signal has a value greater than“Max_Torque_Frequency_LDW”(maximum allowed safe torque), the torque signal “limited_LDW_Torq_Req” shall be set to 0, else“limited_LDW_Torq_Req” shall take the value of “processed_LDW_Torq_Req”.	C	TORQUE_LIMITER	“limited_LDW_Torq_Req” = 0(Nm=Newtonmeter)
Software Safety Requirement 04-03	The “limited_LDW_Torq_Req”shall be transformed into a signal “LDW_Torq_Req” whichis suitable to be transmitted outside of the LDW Safetycomponent (“LDW Safety”) to the “Final EPS Torque”component.	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

Lane Keeping Assistance(LKA) sensor Malfunction Software Requirements:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	The LKA safety component shall ensure that the loss of camera sensor torque request transmission will deactivate the LKA feature and the 'LKA_Torque_Request' shall be	B	50ms	LDW Safety block	Set Lane keeping assistance torque to zero

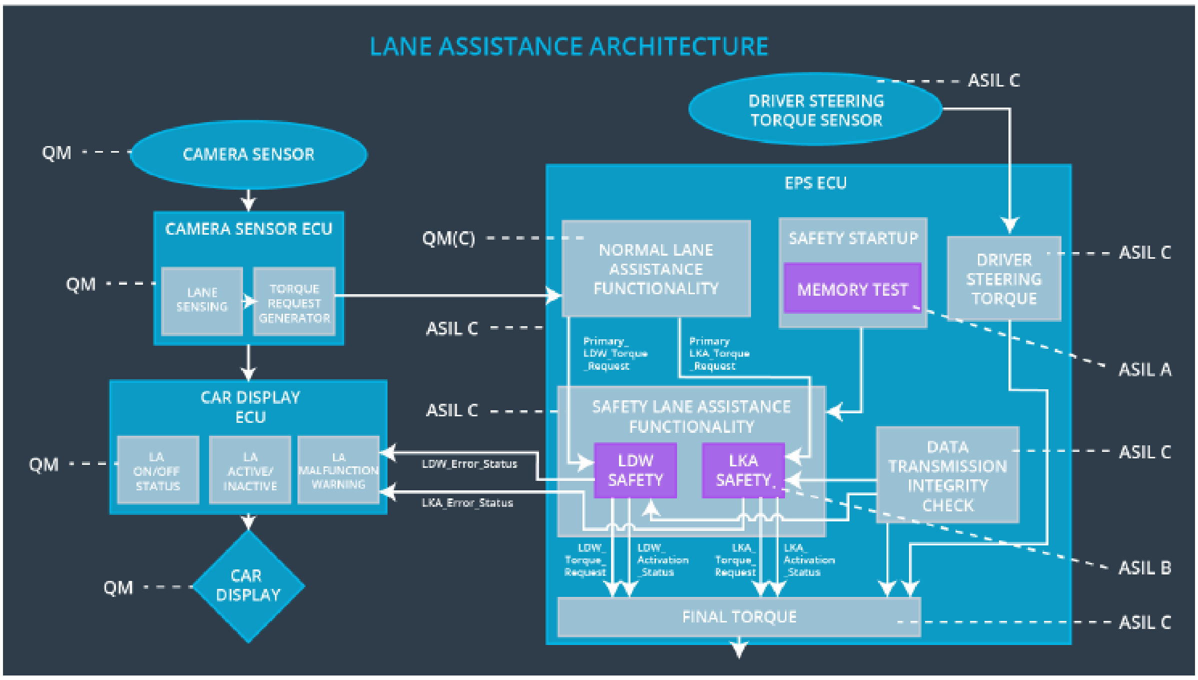
	set to zero.				

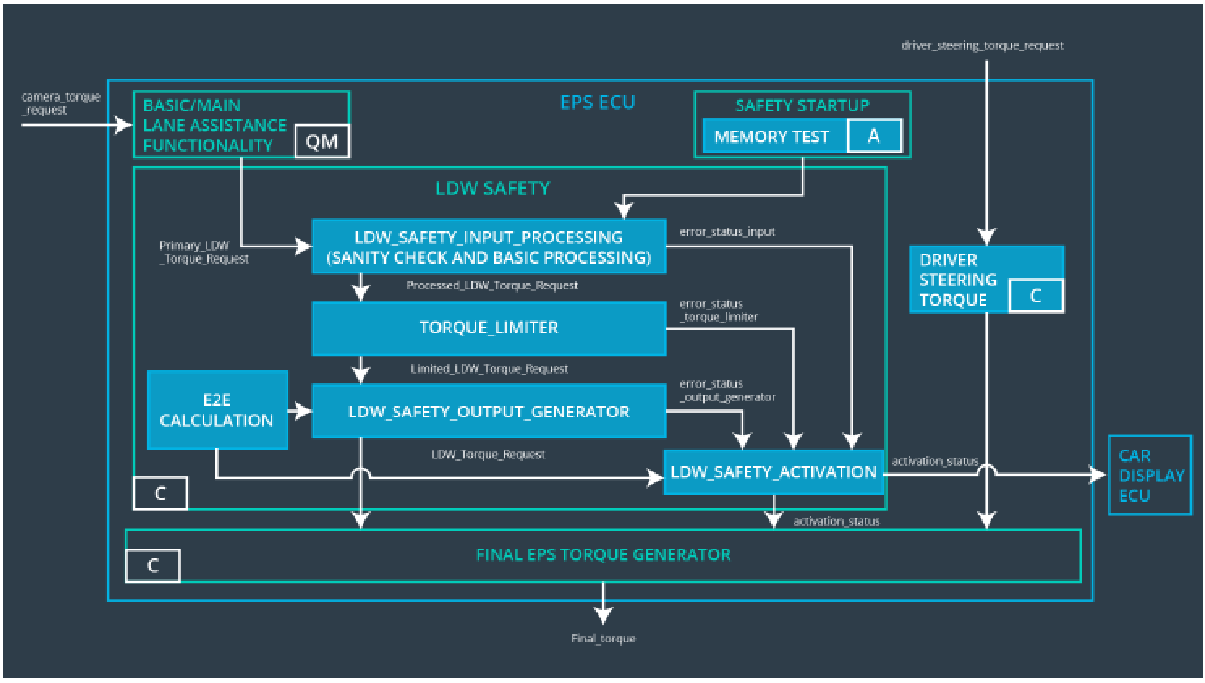

driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LKA SAFETY
Primary_LKA_Torque_Request
LKA_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LKA_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LKA_Torque_Request
E2E CALCULATION
LKA_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LKA_Torque_Request
LKA_SAFETY_ACTIVATION
activation_status
B
DRIVER STEERING TORQUE
C
CAR DISPLAY ECU
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

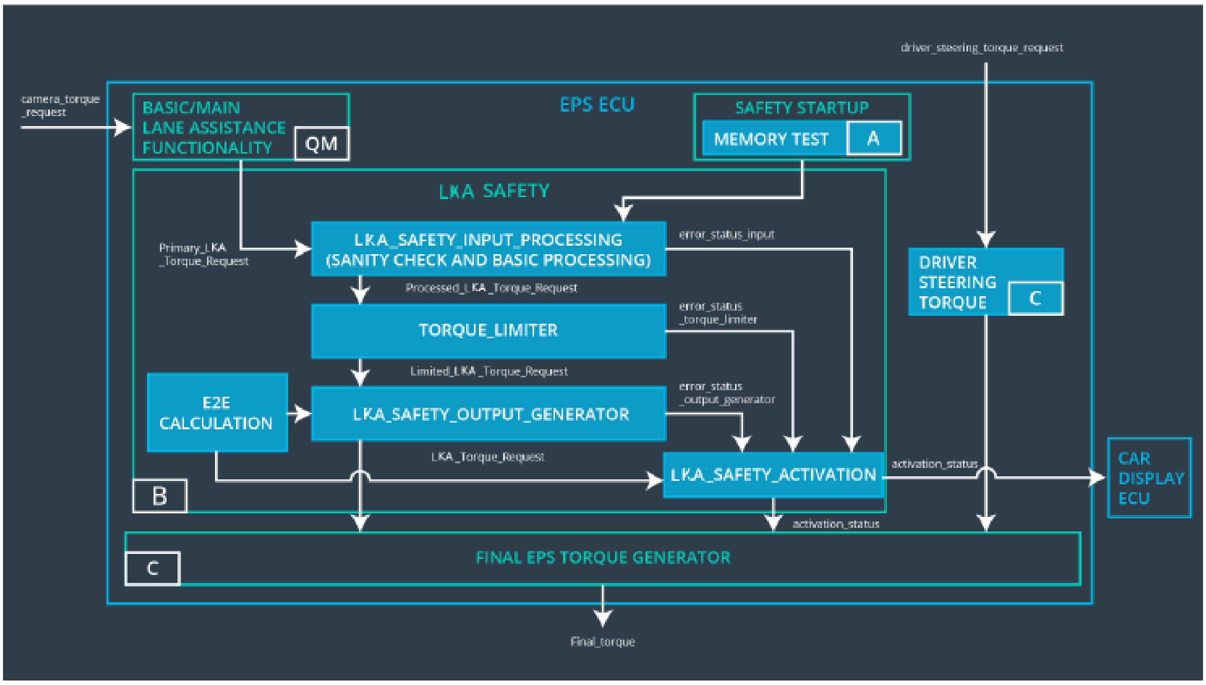
ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 05-01	The input signal "Primary_LKA_Torq_Req" shall be read and pre-processed to determine the torque request coming from the "Basic/Main LA Functionality" SW Component. Signal"processed_LKA_Torq_Re e q" shall be generated at the end of the processing.	B	LKA_SAFETY_INPUT_PROCESSING	Not Applicable
Software Safety Requirement 05-02	In case the "processed_LKA_Torq_Req" signal has an invalid Alive counter (SQC), the camera sensor ECU is no longer detecting lane lines, the torque signal "limited_LKA_Torq_Req" shall be set to 0, else"limited_LKA_Torq_Req" shall take the value of	B	TORQUE_LIMITER	"limited_LKA_Torq_Req" = 0(Nm=Newtonmeter)

	“processed_LKA_Torq_Req”.			
Software Safety Requirement 05-03	The “limited_LKA_Torq_Req”shall be transformed into a signal “LKA_Torq_Req” whichis suitable to be transmitted outside of the LKA Safetycomponent (“ LKA Safety”) to the “Final EPS Torque”component.	B	LKA_SAFETY _OUTPUT_ GENERATOR	LKA_Torq_Req= 0 (Nm)

Refined Architecture Diagram




driver_steering_torque_request
camera_torque _request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW _Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status _torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status _output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque


driver_steering_torque_request
camera_torque _request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LKA SAFETY
Primary_LKA _Torque_Request
LKA_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LKA_Torque_Request
TORQUE_LIMITER
error_status _torque_limiter
Limited_LKA_Torque_Request
E2E CALCULATION
LKA_SAFETY_OUTPUT_GENERATOR
error_status _output_generator
LKA_Torque_Request
LKA_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
B
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque