Elektrobit

UDACITY

Software Safety Requirements and Architecture
Lane Assistance

Document Version: 1.0

Document History

Date	Version	Editor	Description
July 28, 2017	1.0	John Chen	Initial Draft

Table of Contents

Purpose

The purpose of the software safety requirments 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, tailored.

Inputs to the Software Requirements and Architecture Document

Technical safety requirements

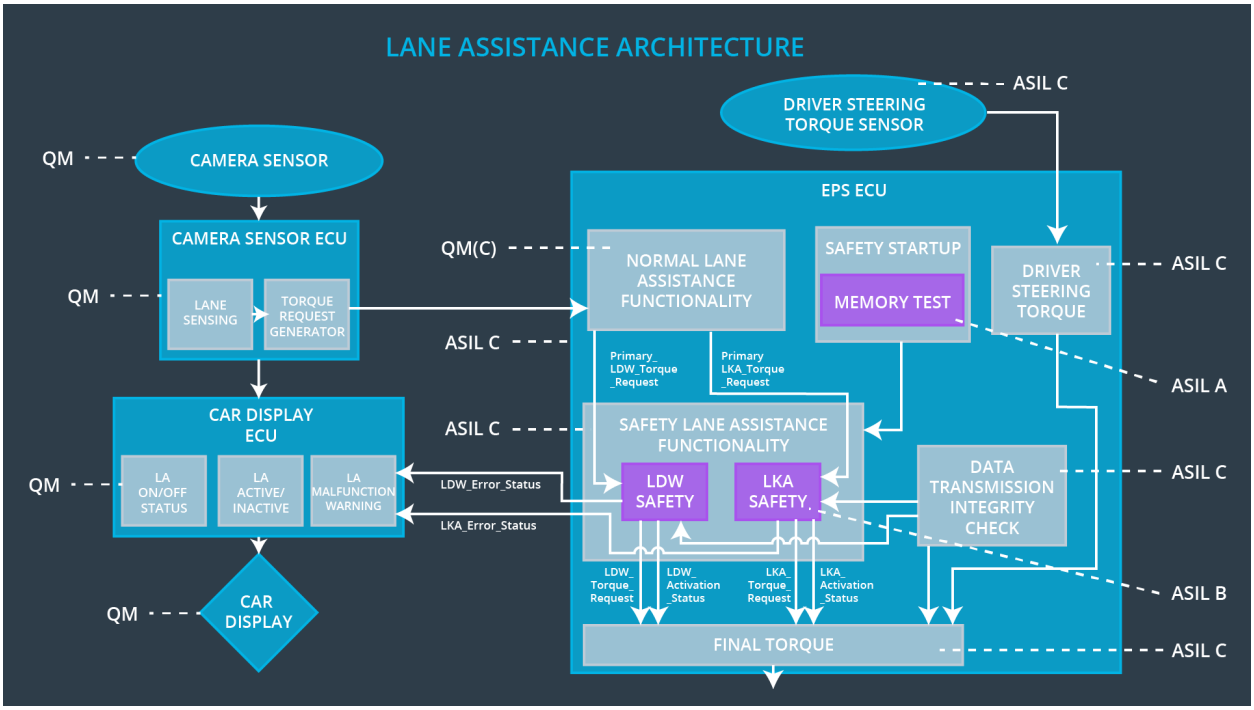
Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01-01-01	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.	C	50 ms	LDW Safety block	Set lane departure warning torque to zero
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.	C	50 ms	LDW Safety block	Set lane departure warning torque to zero
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.	C	50 ms	LDW Safety block	Set lane departure warning torque to zero

Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	LDW Safety block	Set lane departure warning torque to zero
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.	A	Ignition cycle	Data Transmission Integrity Check	Set lane departure warning torque to zero
Technical Safety Requirement 01-02-01	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	50 ms	LDW Safety block	Set lane departure warning torque to zero
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure that the duration of the lane keeping assistance torque applied is less than Max_Duration.	C	500 ms	LKA Safety block	Set lane keeping assistance torque to zero
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.	C	500 ms	LKA Safety block	Set lane keeping assistance torque to zero
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.	C	500 ms	LKA Safety block	Set lane keeping assistance torque to zero
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500 ms	LKA Safety block	Set lane keeping assistance torque to zero

Technical Safety Requirement 02-01-05	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	Set lane keeping assistance torque to zero
Technical Safety Requirement 02-02-01	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 set to zero.	C	500 ms	LKA Safety block	Set lane keeping assistance torque to zero

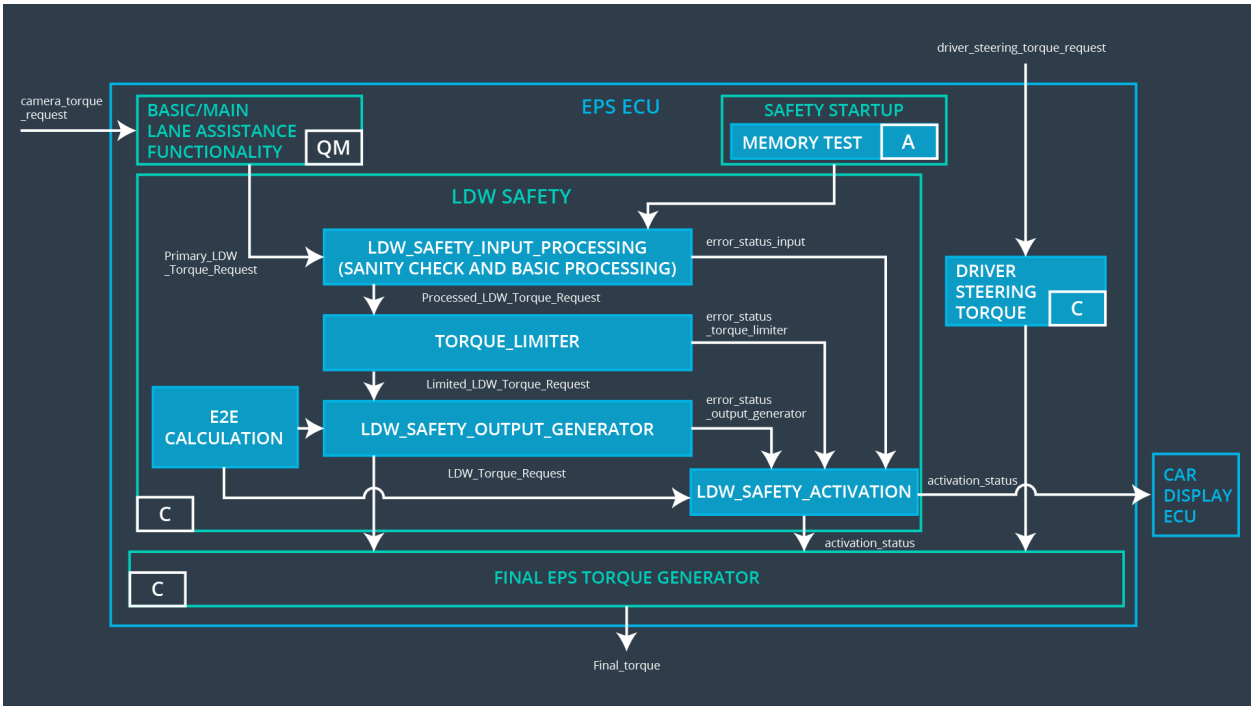
Refined Architecture Diagram from the Technical Safety Concept



Software Requirements

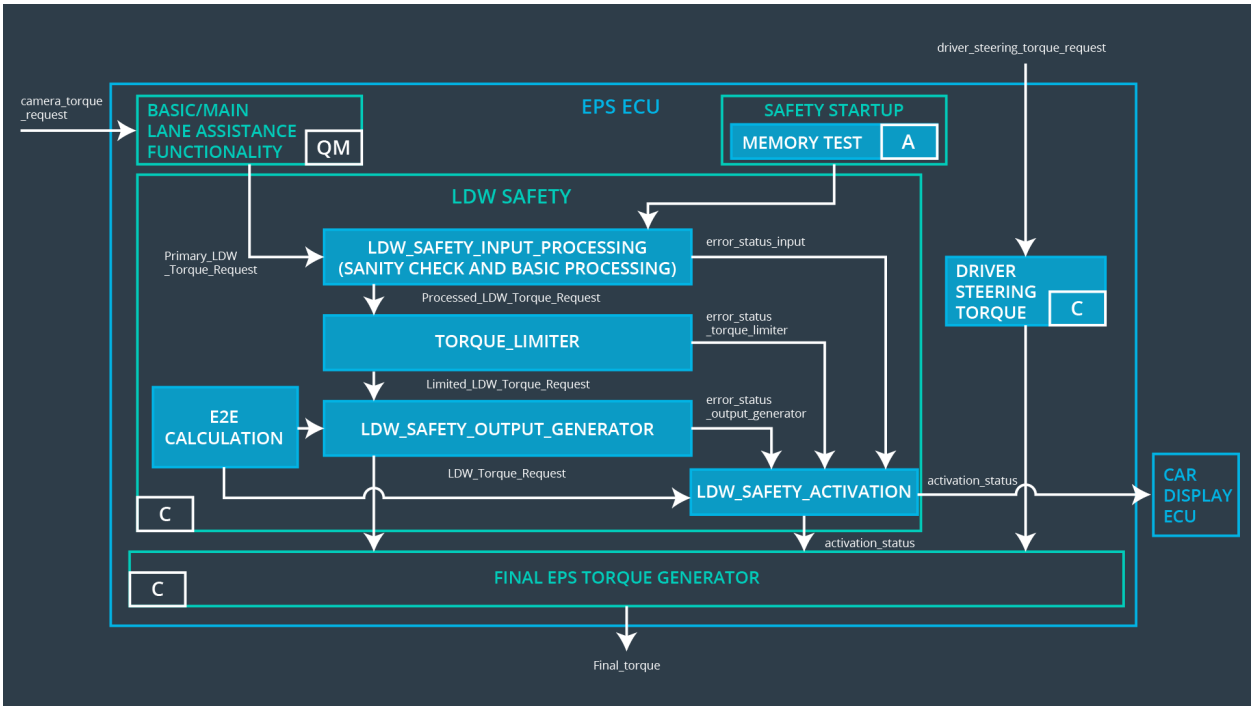
Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
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	C	50 ms	LDW Safety block	Set lane departure warning torque to zero



ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-01-01	The input signal “Primary_LDW_Torq_Req” shall be read and pre-processed to 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.	C	LDW_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 01-01-01-02	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=Newton-meter)
Software Safety Requirement 01-01-01-03	The “limited_LDW_Torq_Req”shall be transformed into a signal “LDW_Torq_Req” whichis suitable to be transmittedoutside of the LDW Safetycomponent (“LDW Safety”) to the “Final EPS Torque”component. Also see SofSafReq 01-02-01-03	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

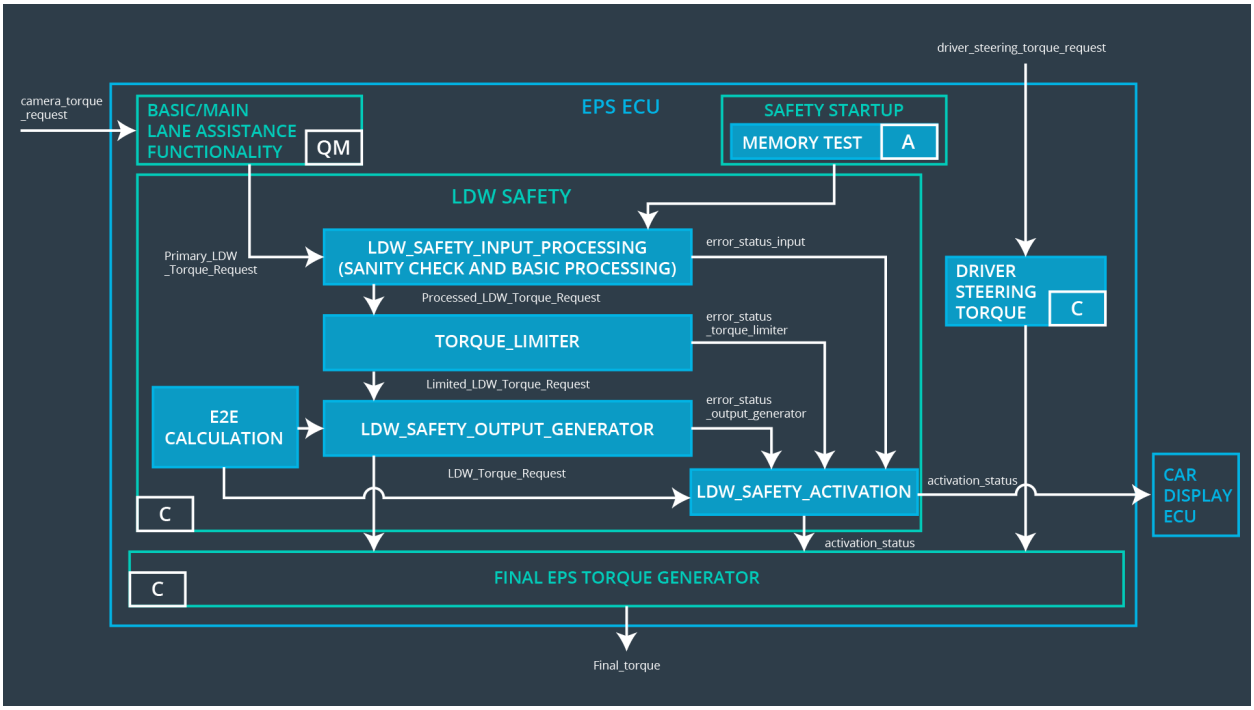
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-02	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW_Torque_Request shall be set to zero	C	50 ms	LDW Safety block	Set lane departure warning torque to zero



ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-02-01	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	N/A

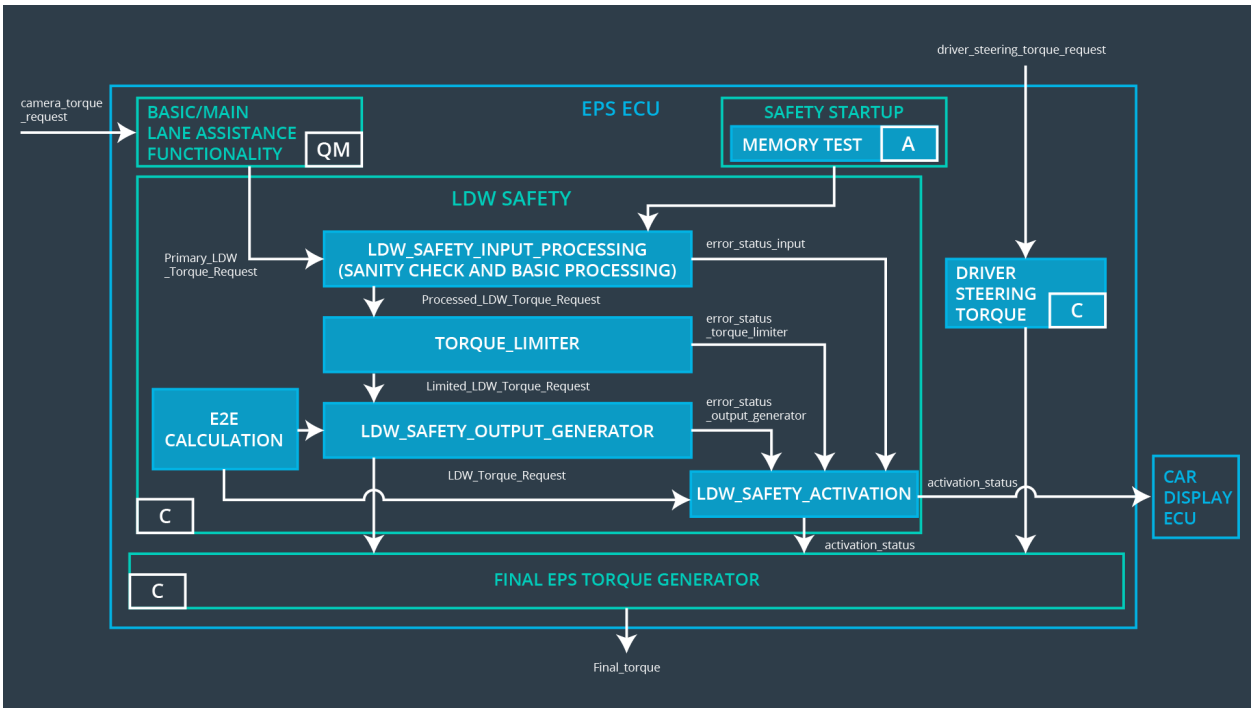
	QUE_LIMITER), error_status_output_gen(LDW_SAFETY_OUTPUT_GENERATOR)			
Software Safety Requirement 01-01-02-02	A software element shall evaluate the error status of all the other software elements and in case any 1 of them indicates an error, it shall deactivate theLDW feature(“activation_status”=0)	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)
Software Safety Requirement 01-01-02-03	In case of no errors from the software elements, the status of the LDW feature shall be set to activated (“activation_status”=1)	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement 01-01-02-04	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	C	All	LDW_Torq_Req= 0 (Nm)
Software Safety Requirement 01-01-02-05	Once the LDW functionality has been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again.		LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-03	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	50 ms	LDW Safety block	Set lane departure warning torque to zero



ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-03-01	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	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	Data Transmission Integrity Check	N/A



ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-04-01	Any data to be transmitted outside of the LDW Safetycomponent (“LDW Safety”)including "LDW_Torque_Req"and “activation_status” (seeSofSafReq 01-01-02-02)	C	E2ECalc	LDW_Torq_Req = 0 (Nm)

	shall beprotected by an End2End(E2E)protection mechanism			
Software Safety Requirement 01-01-04-02	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)

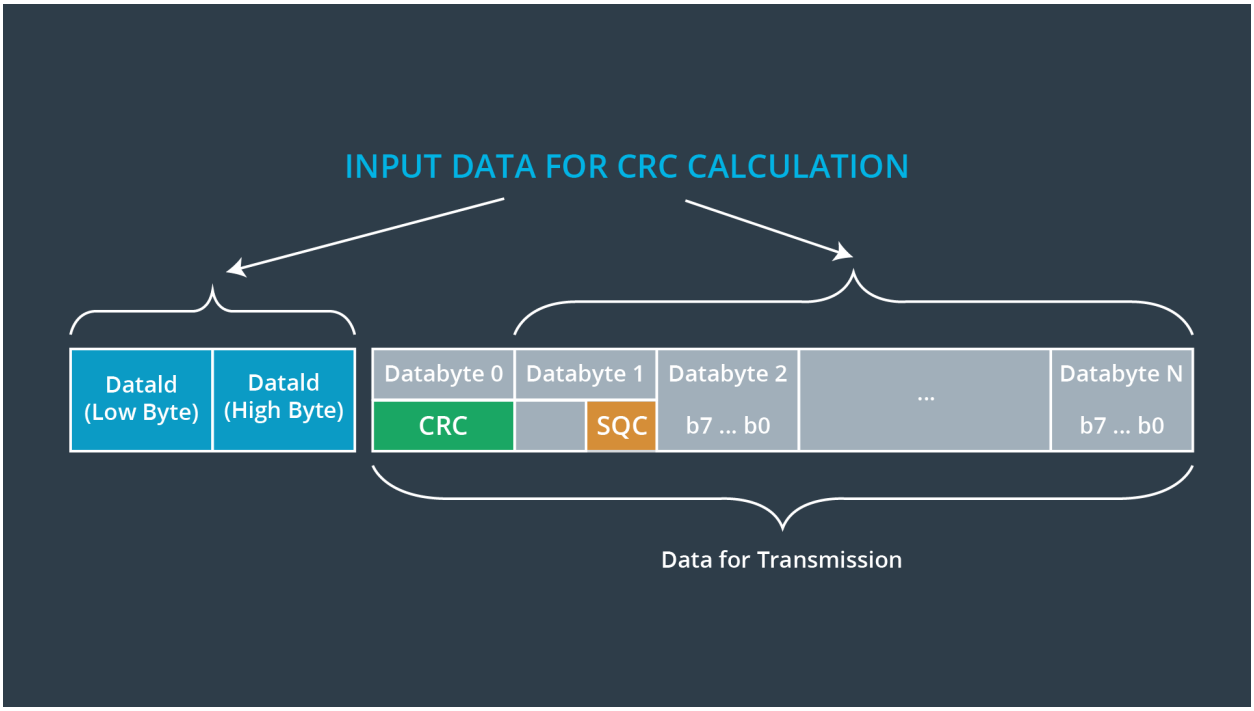
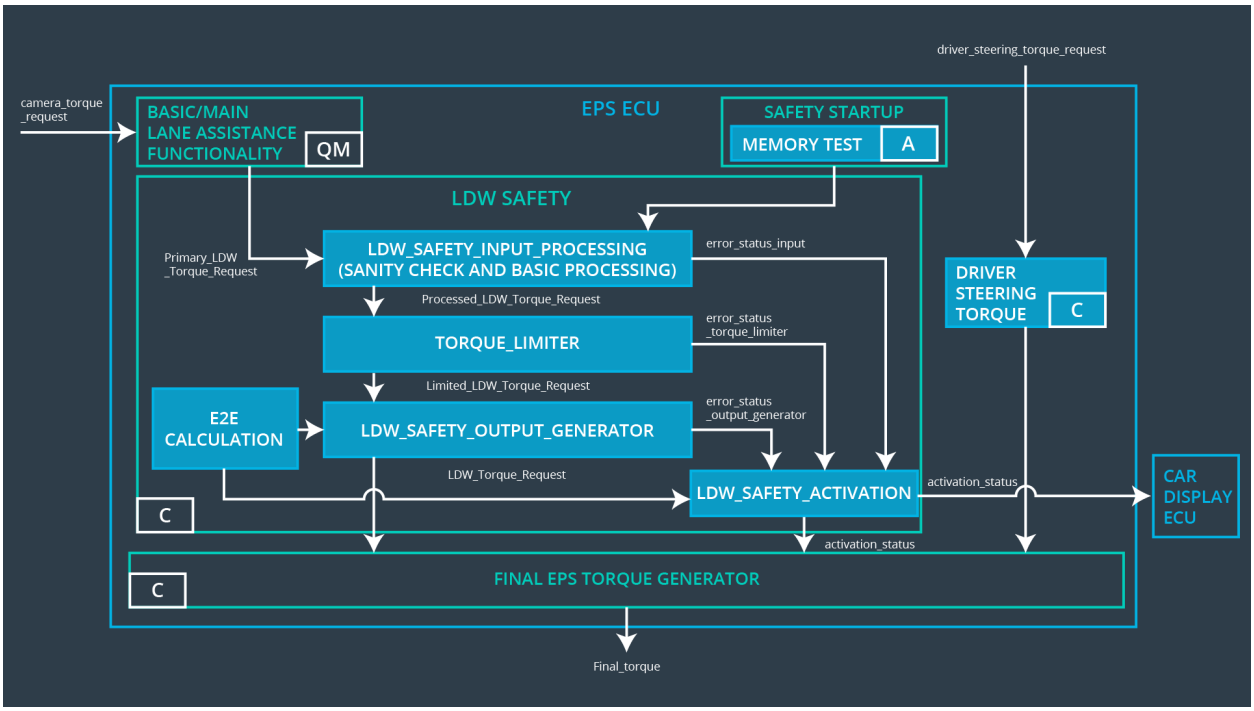


Figure 1: Example E2E Protocol with CRC (Cyclical Redundancy Check) and SQC (Sequence Counter)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
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	A	Ignition cycle	Data Transmission Integrity Check	Set lane departure warning torque to zero

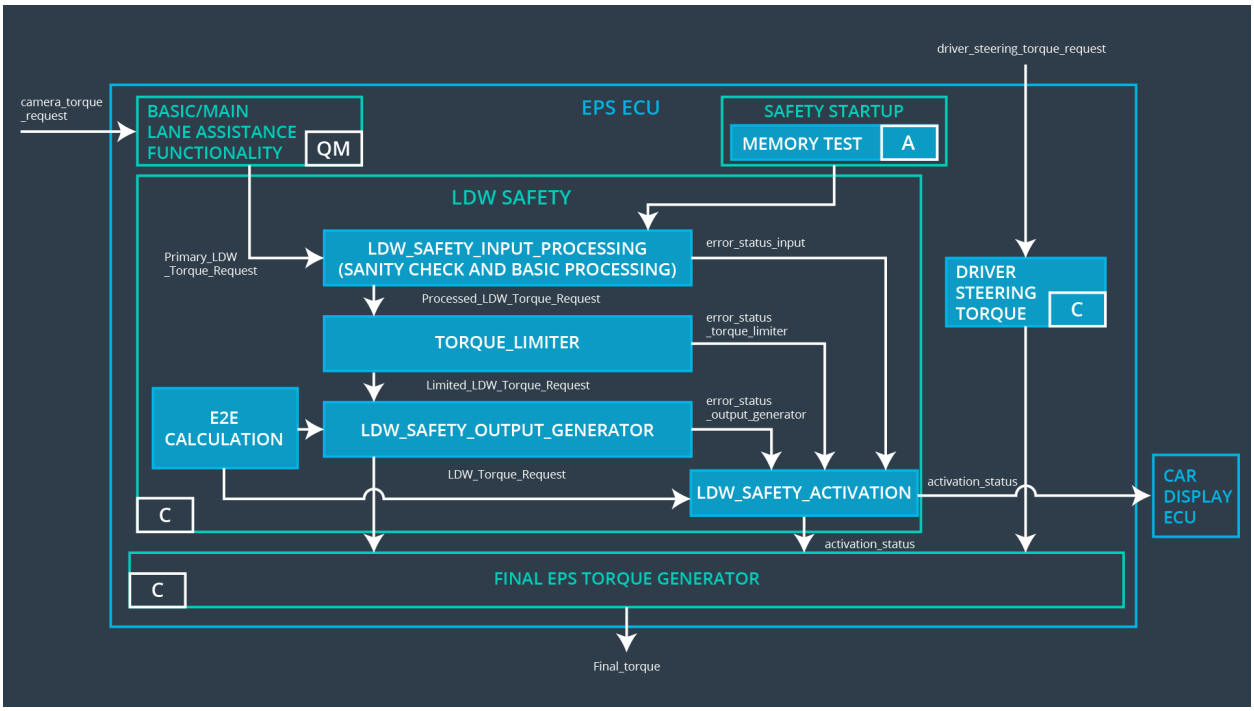


ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-05-01	A CRC verification check over the software code in the Flash memory shall be done every time the ignition is switched from off to on to check for any corruption of content.	A	MEMORYTEST	Activation_status = 0
Software	Standard RAM tests to check	A	MEMORYTES	Activation_status = 0

Safety Requirement 01-01-05-02	the data bus, address bus and device integrity shall be done every time the ignition is switched from off to on (E.g.walking 1s test, RAM pattern test. Refer RAM and processor vendor recommendations)		T	
Software Safety Requirement 01-01-05-03	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 01-01-05-04	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 the LDW functionality is deactivated and the LDWTorque is set to 0	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

Lane Departure Warning (LDW) Fequency Malfunction Software Requirements:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
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	C	50 ms	LDW Safety block	Set lane departure warning torque to zero

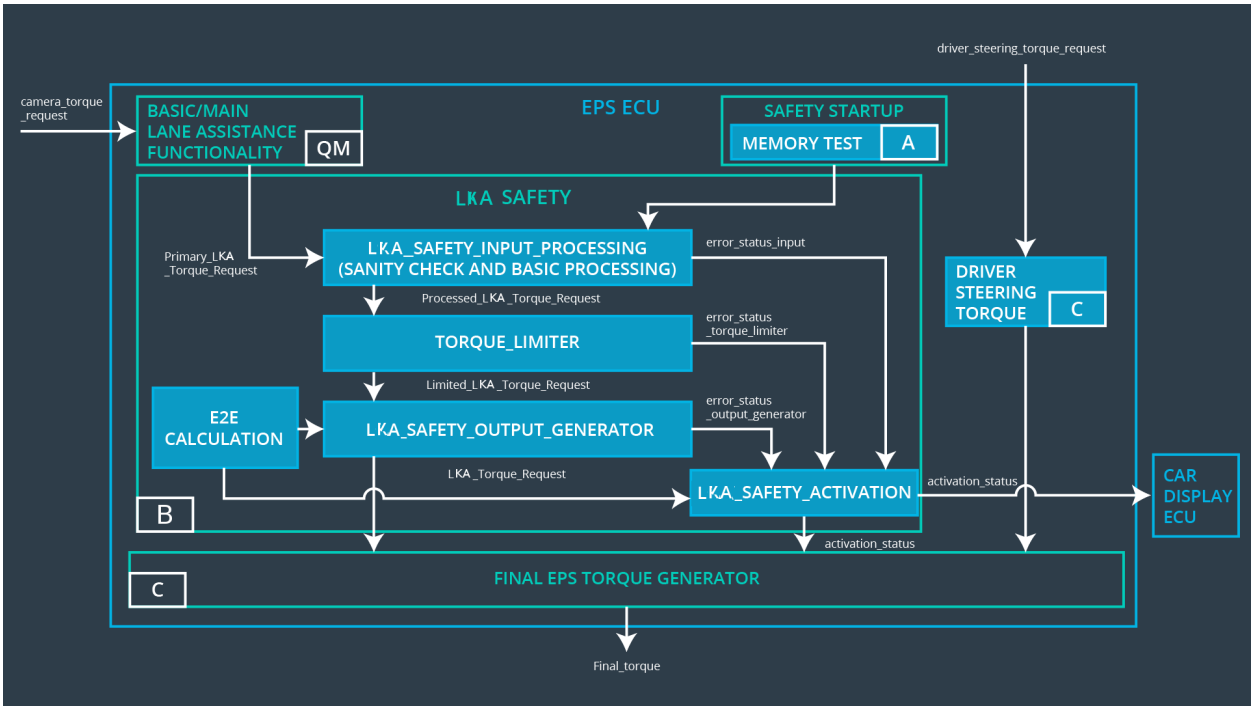


ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State

Software Safety Requirement 01-02-01-01	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	N/A
Software Safety Requirement 01-02-01-02	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=Newton-meter)
Software Safety Requirement 01-02-01-03	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. Also see SofSafReq 01-01-01-03, 02-01-01-03 and 02-02-01-03.	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

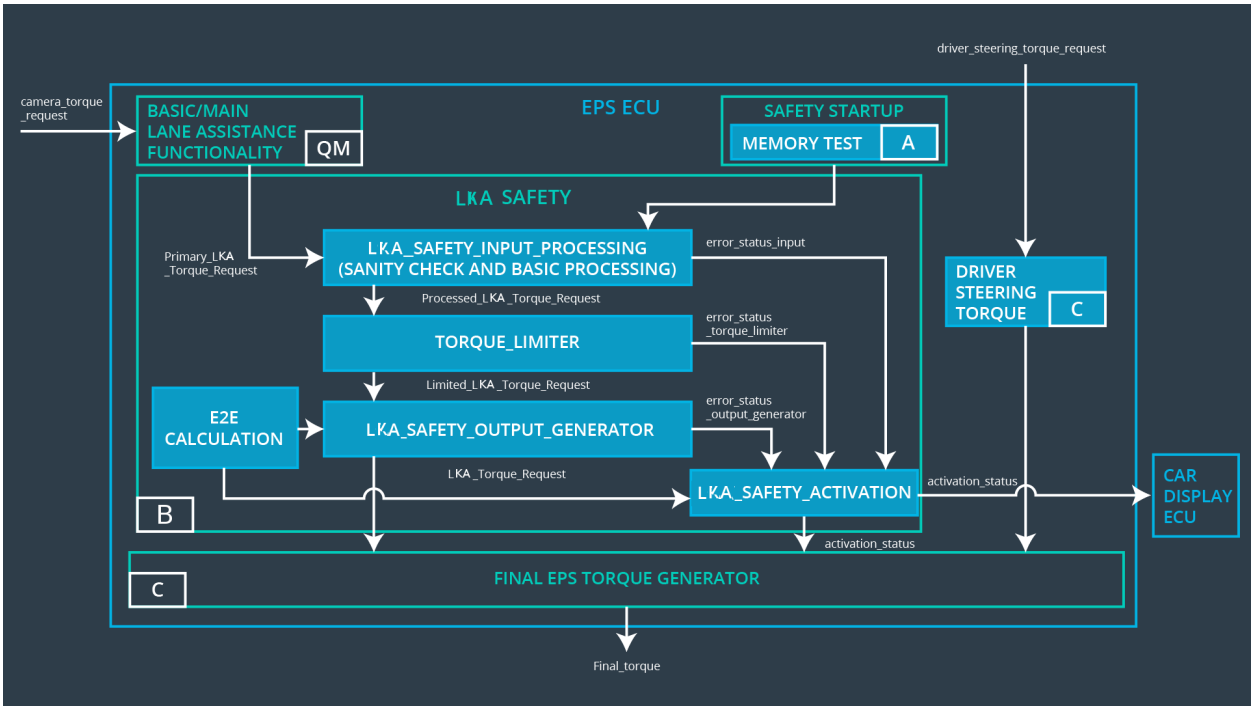
Lane Keeping Assistance (LKA) Max Duration Malfunction Software Requirements:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure that the duration of the lane keeping assistance torque applied is less than Max_Duration.	B	500 ms	LKA Safety block	Set lane keeping assistance torque to zero



ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01-01-01	The input signal “Primary_LKA_Torq_Req” shall be read and pre-processed to determine the torque request coming from the “Basic/Main LAFunctionality” SW Component. Signal“processed_LKA_Torq_Req”shall be generated at the end of the processing.	B	LDW_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 02-01-01-02	In case the “processed_LKA_Torq_Req” signal is not zero the “applied_counter” will be incremented by the time interval passed since last application, else the “applied_counter” will be set to zero. If “applied_counter” is more than “MAX_Duration,” (maximum allowed duration to apply lane keeping assistance torque), the torque signal “limited_LKA_Torq_Req” shall be set to 0, else“limited_LKA_Torq_Req” shall take the value of “processed_LKA_Torq_Req”.	B	TORQUE_LIMITER	“limited_LKA_Torq_Req” = 0(Nm=Newton-meter)
Software Safety Requirement 02-01-01-03	The “limited_LKA_Torq_Req”shall be transformed into a signal “LDW_Torq_Req” whichis suitable to be transmittedoutside of the LDW Safetycomponent (“LDW Safety”) to the “Final EPS Torque”component. Also see SofSafReq 01-01-01-03 and 01-02-01-03	B	LDW_SAFETY_OUTPUT_GENERATOR	LKA_Torq_Req= 0 (Nm)

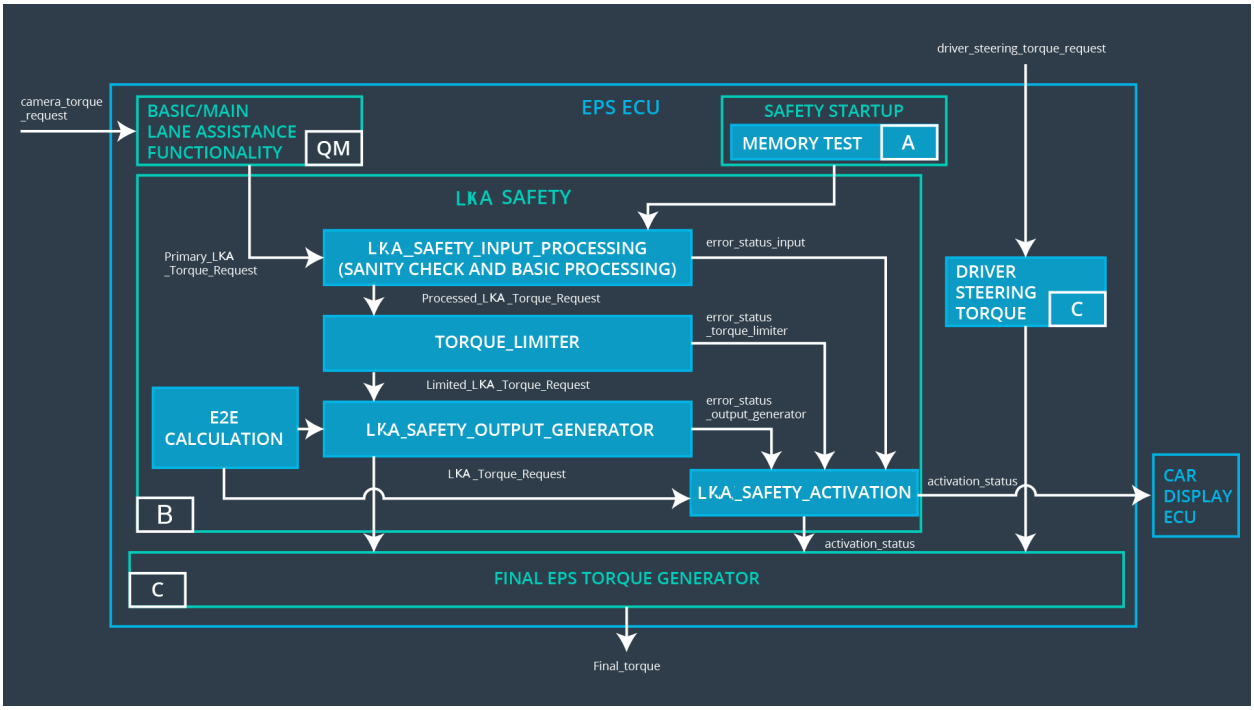
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-01-02	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the LKA_Torque_Request shall be set to zero	B	500 ms	LKA Safety block	Set lane keeping assistance torque to zero



ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01-02-01	Each of the SW elements shall output a signal to indicate any error which is detected by the element. Error signal = error_status_input(LKA_SAFETY_INPUT_PROCESSING), error_status_torque_limiter(TOR	B	All	N/A

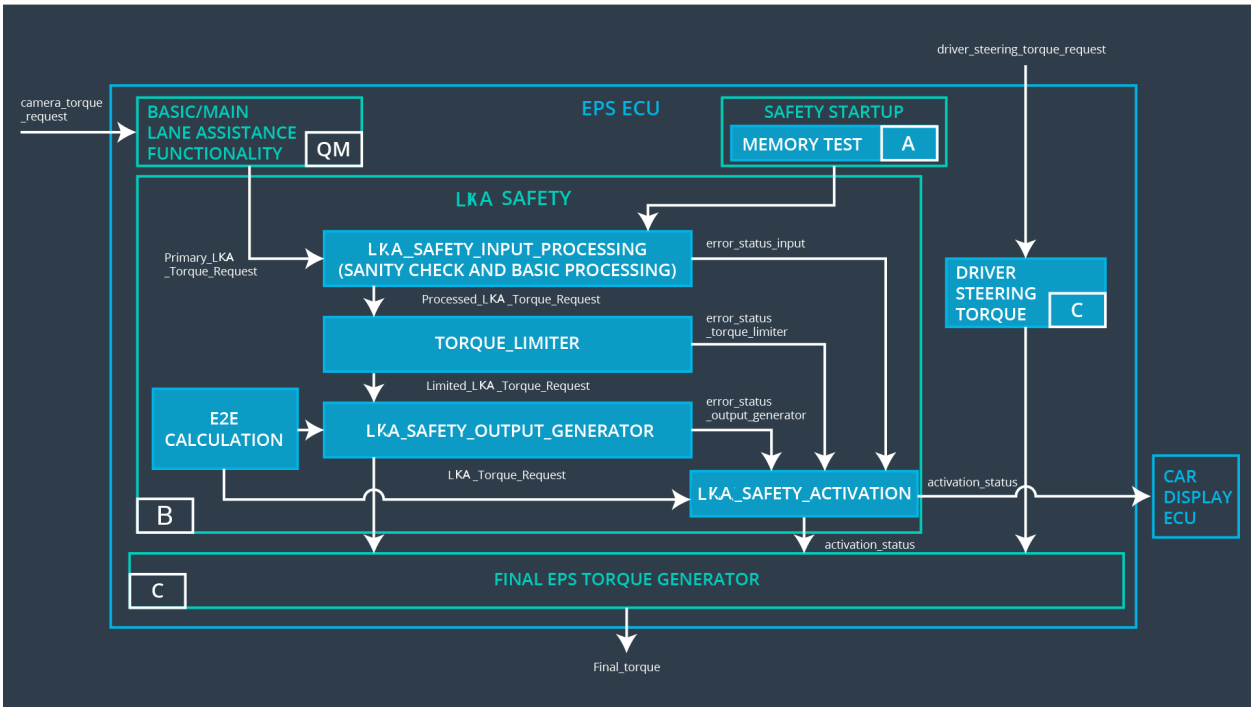
	QUE_LIMITER), error_status_output_gen(LKA_SAFETY_OUTPUT_GENERATOR)			
Software Safety Requirement 02-01-02-02	A software element shall evaluate the error status of all the other software elements and in case any 1 of them indicates an error, it shall deactivate the LKA feature(“activation_status”=0)	B	LKA_SAFETY_ACTIVATION	Activation_status = 0 (LKA function deactivated)
Software Safety Requirement 02-01-02-03	In case of no errors from the software elements, the status of the LDW feature shall be set to activated (“activation_status”=1)	B	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement 02-01-02-04	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 “LKA_Torq_Req” is set to 0	B	All	LKA_Torq_Req= 0 (Nm)
Software Safety Requirement 02-01-02-05	Once the LKA functionality has been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again.		LKA_SAFETY_ACTIVATION	Activation_status = 0 (LKA function deactivated)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-01-03	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	500 ms	LKA Safety block	Set lane keeping assistance torque to zero



ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01-03-01	When the LKA function is deactivated (activation_status set to 0), the activation_status shall be sent to the car displayECU.	B	LKA_SAFETY_ACTIVATION, CarDisplay ECU	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for LKA_Torque_Request signal shall be ensured	B	500 ms	Data Transmission Integrity Check	N/A



ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01-04-01	Any data to be transmitted outside of the LKA Safetycomponent (“LKA Safety”)including "LKA_Torque_Req"and “activation_status” (seeSofSafReq 02-01-02-02)	B	E2ECalc	LKA_Torq_Req = 0 (Nm)

	shall beprotected by an End2End(E2E)protection mechanism			
Software Safety Requirement 02-01-04-02	The E2E protection protocol shall contain and attach the control data: alive counter (SQC) and CRC to the data to be transmitted.	B	E2ECalc	LKA_Torq_Req = 0 (Nm)

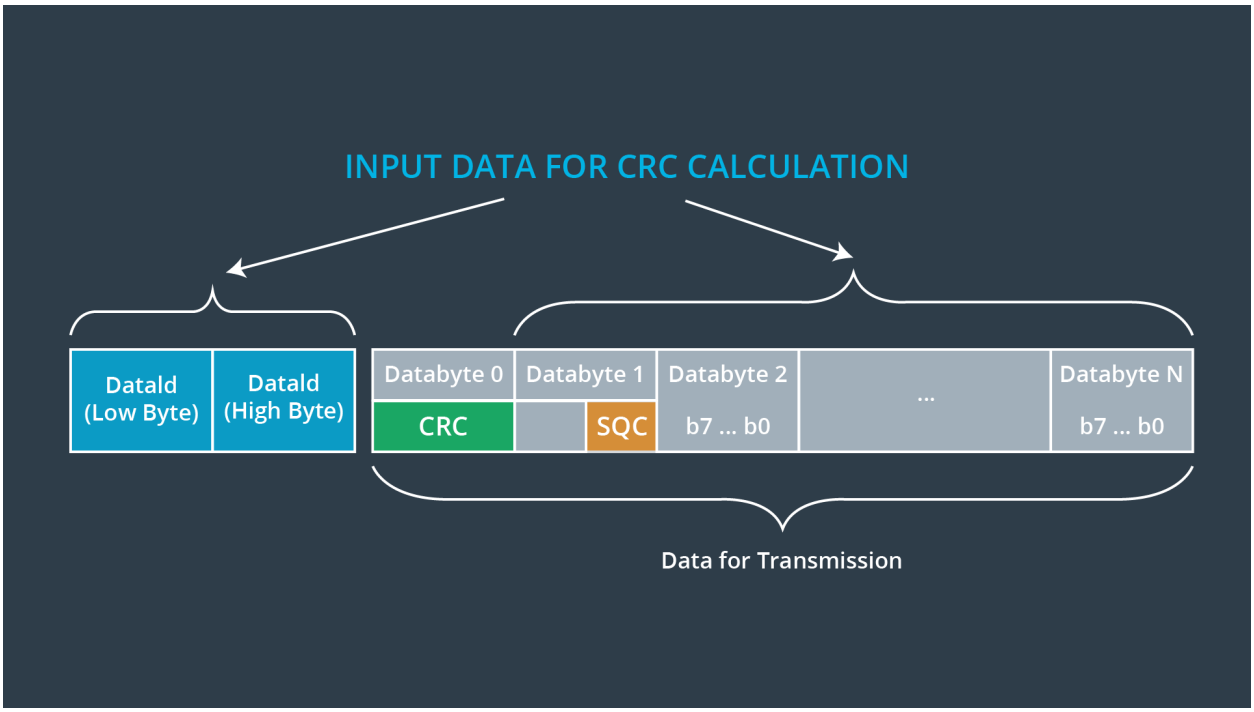
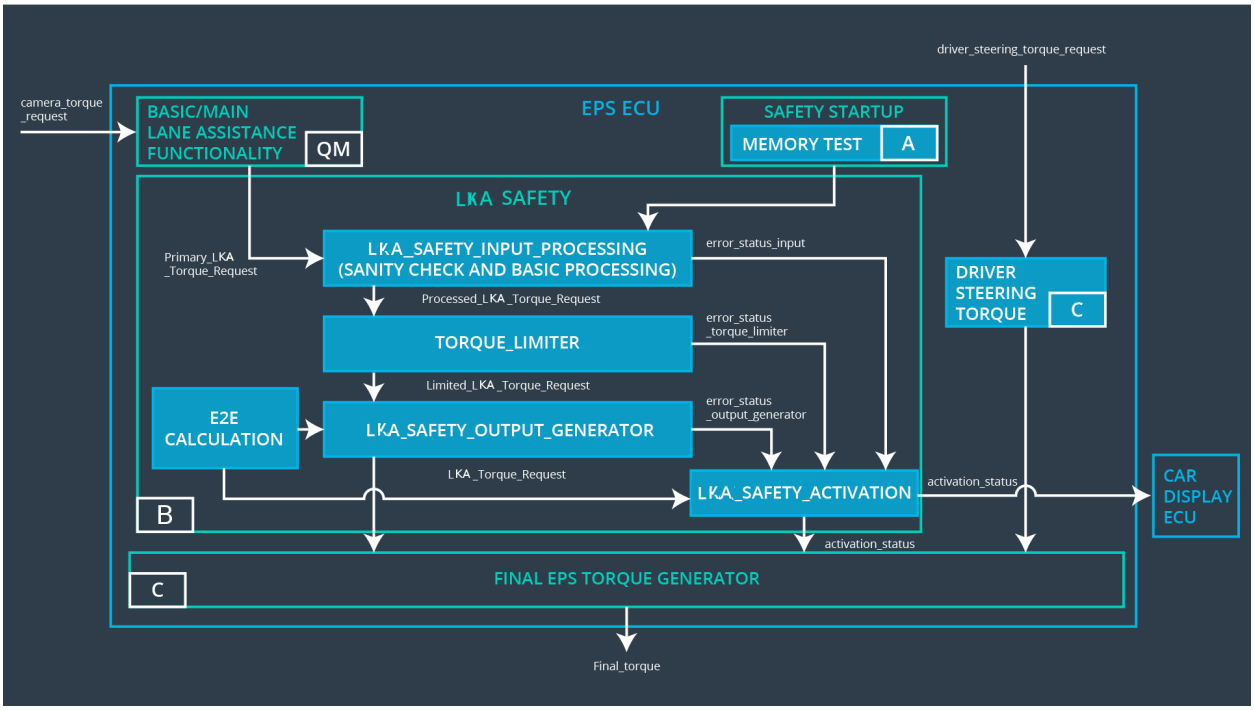


Figure 2: Example E2E Protocol with CRC (Cyclical Redundancy Check) and SQC (Sequence Counter)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-01-05	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	Set lane keeping assistance torque to zero

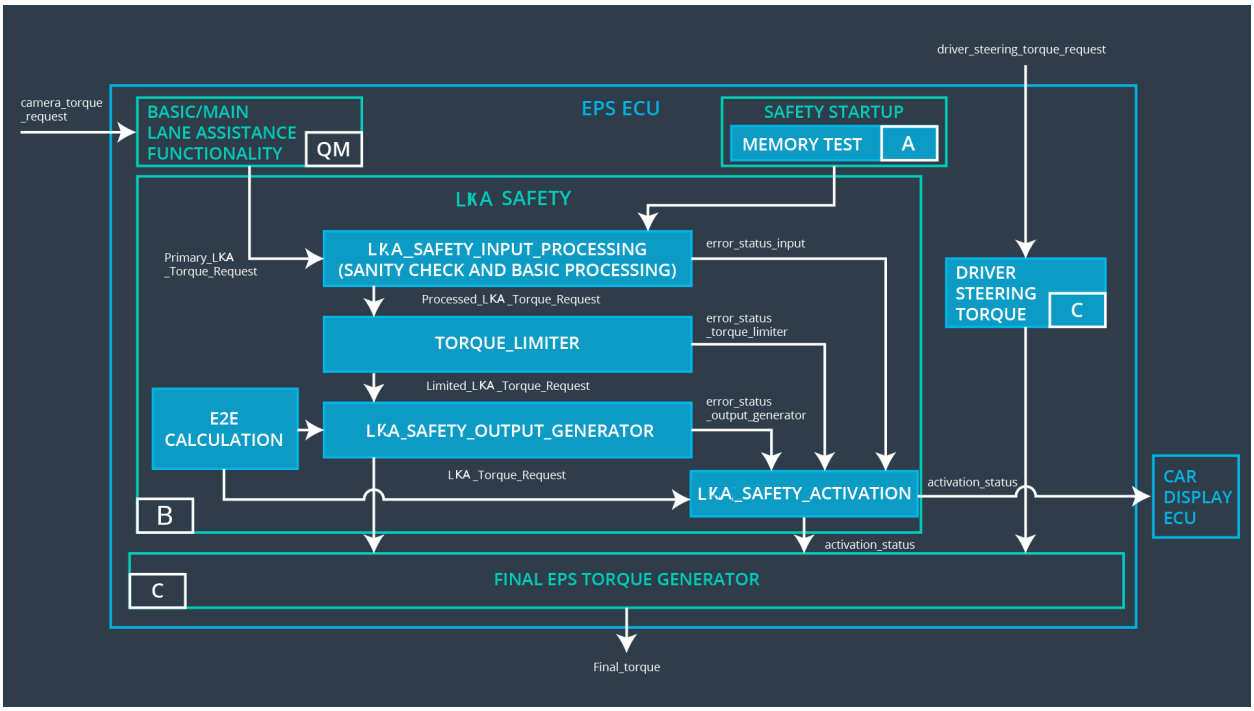


ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01-05-01	A CRC verification check over the software code in the Flash memory shall be done every time the ignition is switched from off to on to check for any corruption of content.	A	MEMORYTEST	Activation_status = 0
Software	Standard RAM tests to check	A	MEMORYTES	Activation_status = 0

Safety Requirement 02-01-05-02	the data bus, address bus and device integrity shall be done every time the ignition is switched from off to on (E.g.walking 1s test, RAM pattern test. Refer RAM and processor vendor recommendations)		T	
Software Safety Requirement 02-01-05-03	The test result of the RAM or Flash memory shall be indicated to the LKA_Safety component via the “test_status” signal	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 02-01-05-04	In case any fault is indicated via the “test_status” signal the INPUT_LKA_PROCESSING shall set an error on error_status_input (=1) so that the LKA functionality is deactivated and the LDWTorque is set to 0	A	LKA_SAFETY_INPUT_PROCESSING	Activation_status = 0

Lane Keeping Assistance (LKA) Sensor Malfunction Software Requirements:

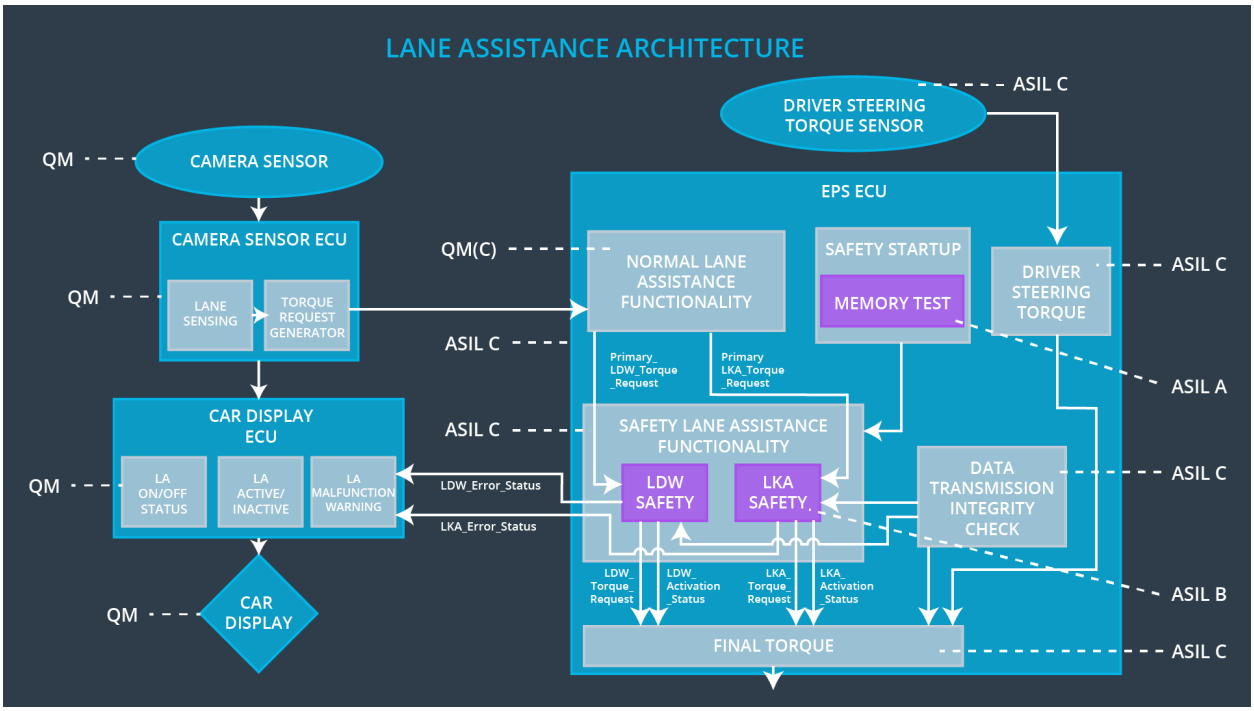
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-02-01	The LKA safety component shall ensure that the loss of camera sensor torque request transmission will deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	B	500 ms	LDW Safety block	Set lane keeping assistance torque to zero

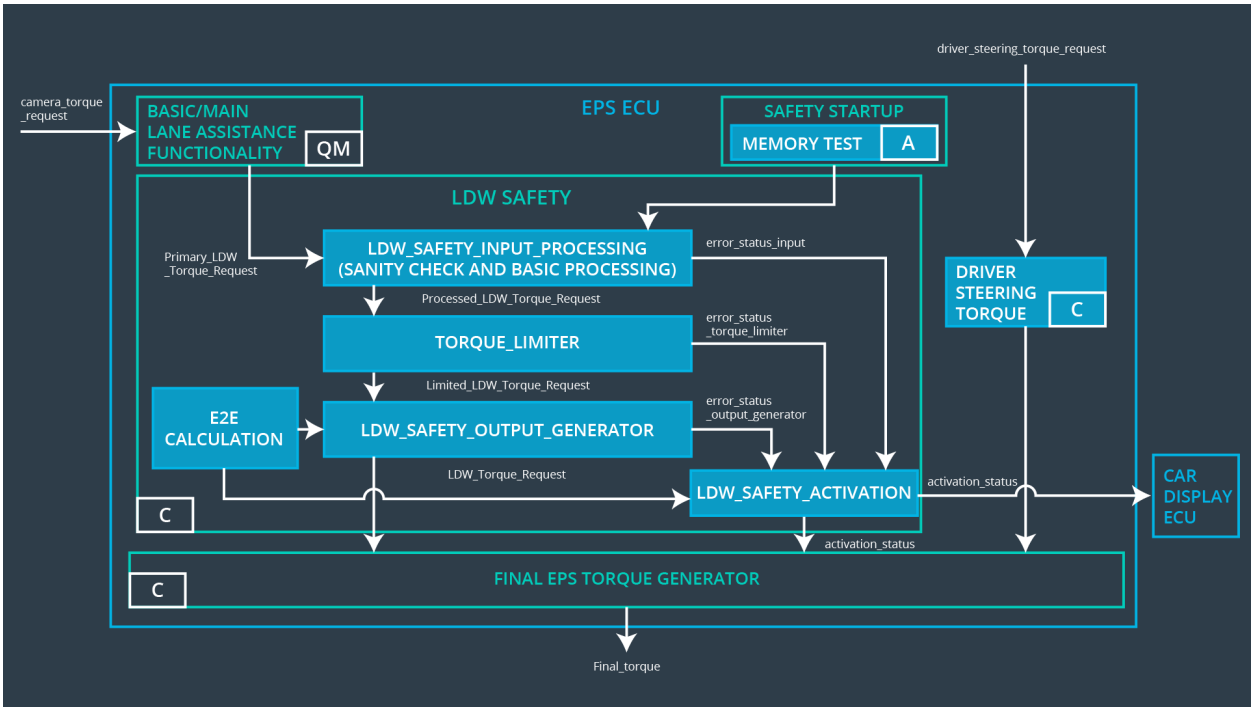


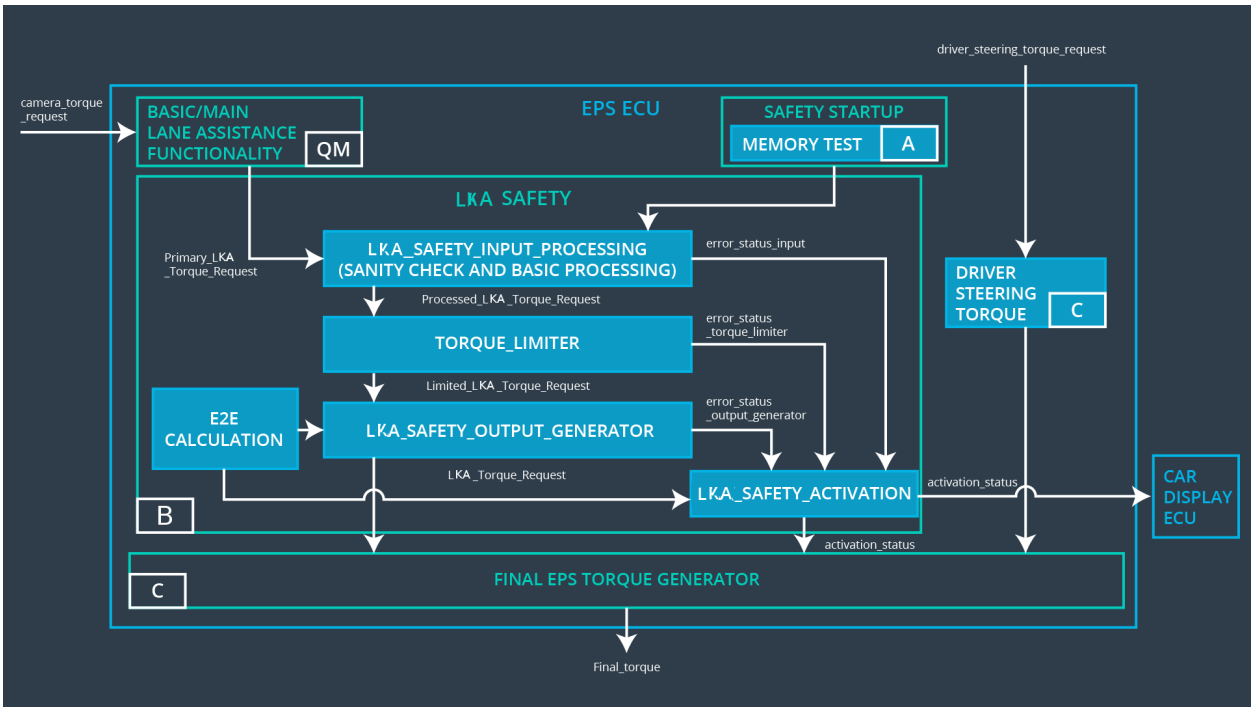
ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State

Software Safety Requirement 02-02-01-01	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_Req” shall be generated at the end of the processing.	B	LKA_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 02-02-01-02	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 “processed_LKA_Torq_Req”.	B	TORQUE_LIMITER	“limited_LKA_Torq_Req” = 0(Nm=Newton-meter)
Software Safety Requirement 02-02-01-03	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. Also see SofSafReq 01-01-01-03, 01-02-01-03 and 02-01-01-03.	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
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
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque
DRIVER
STEERING
TORQUE
C
CAR
DISPLAY
ECU