Elektrobit

UDACITY

Software Safety Requirements and Architecture

Lane Assistance

Document Version: 2.1
Released on 2017-09-17

Document history

Date	Version	Editor	Description
Sep 11, 2017	1.0	Sampath Vanimisetti	Initial draft.
Sep 16, 2017	2.0	Sampath Vanimisetti	Modified software requirements section.
Sep 17, 2017	2.1	Sampath Vanimisetti	Minor changes to figures and diagrams.

Table of Contents

Contents

Purpose

The purpose of the software safety requirements and architecture document is to utilize the technical safety requirements (that were derived from functional safety requirements) and identify detailed software requirements for each line item. These software requirements are then allocated to individual elements of the architecture diagram. In the following, the software requirements for LDW and LKA functions of the lane assistance item will be derived to manage potential malfunctions of the electronic systems as defined by ISO 26262.

Inputs to the Software Requirements and Architecture Document

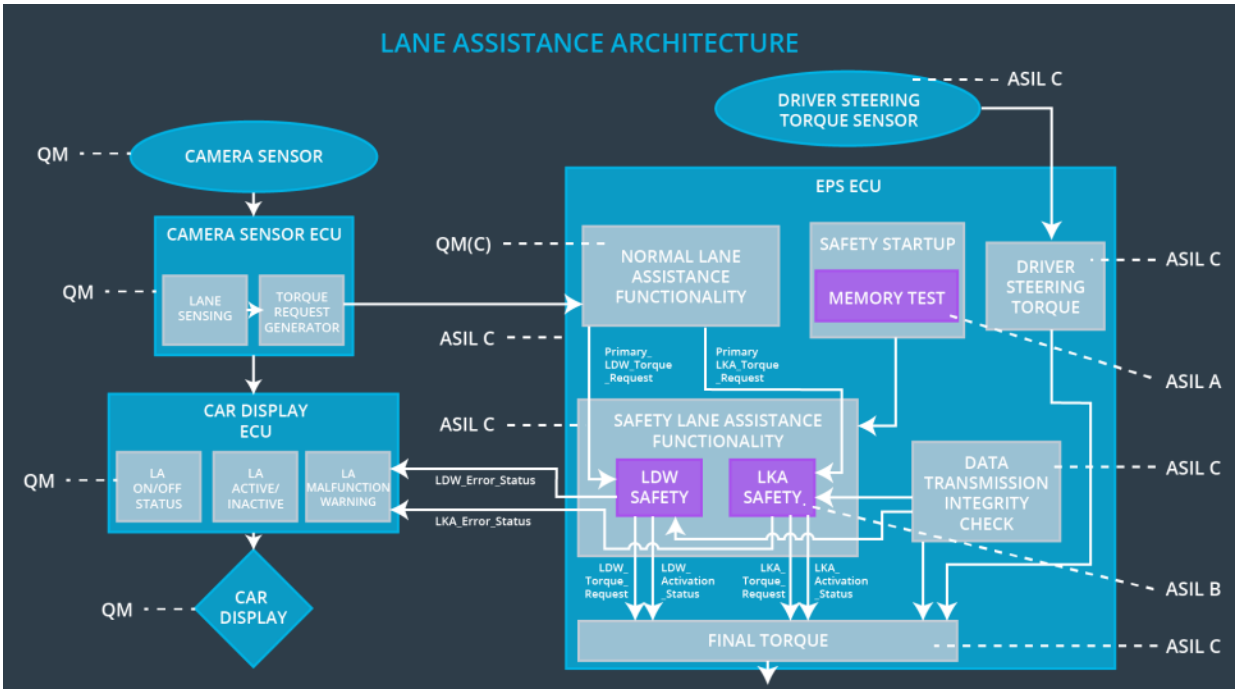
Technical Safety Requirements for Lane Assistance Item:

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 0 & 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
Technical Safety Requirement 02-a	LKA component to ensure that duration of torque assist is less than MAX_LKAStrTrqDuration	C	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 .	C	50 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	C	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	C	50 ms	LKA Safety Block	Set LKA torque to zero

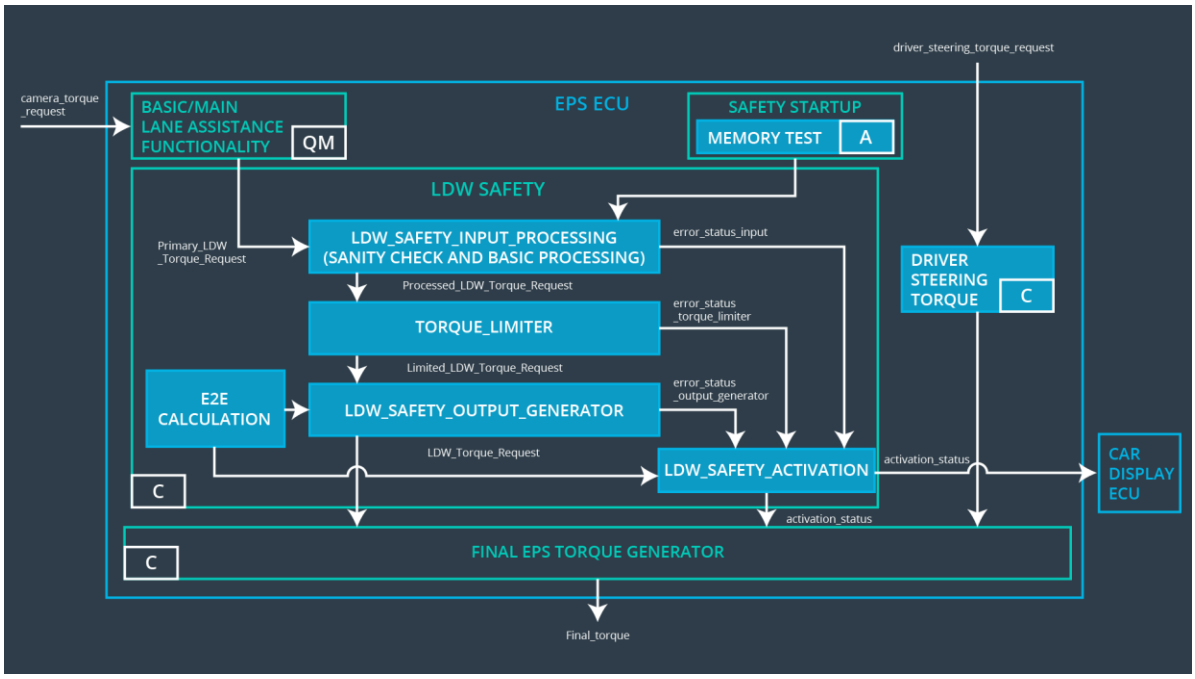
Refined Architecture Diagram from the Technical Safety Concept

The refined architecture of the lane assistance item after technical safety concept analysis and allocation of technical requirements to elements of the architecture is shown below.



Software Requirements

For the following technical safety requirement, software requirements are identified and allocated the architecture diagram in the following manner.



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	C	50 ms	LDW Safety Block	Set LDW torque amp & freq to zero.

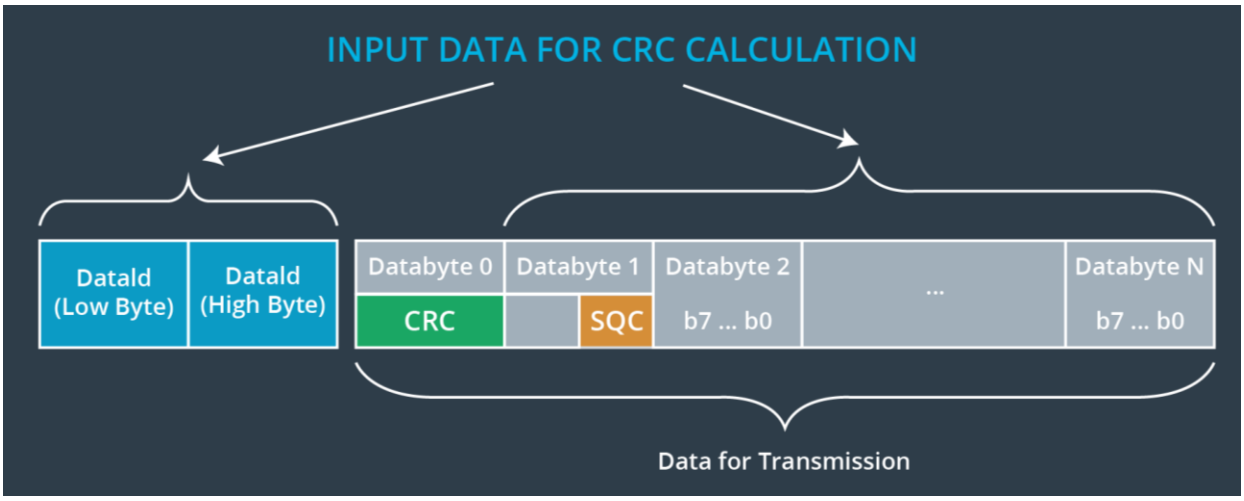
	EPS ECU is below MAX_StrOscTrqAmp and MAX_StrOscTrqFrq				
Technical Safety Requirement 01-d	When failure is detected, disable LDW, set LDW_TrqReq to 0 and send signal to display ECU to turn on the LDW warning light	C	50 ms	LDW Safety	LDW torque output is set to zero

Software requirements for LDW Technical Safety Requirement 01-a:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-a-i	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 01-a-ii	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 (E.g. waking 1s test, RAM pattern test. Refer RAM and processor vendor recommendations)	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 01-a-iii	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-a-iv	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 LDW Torque is set to 0	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

Software requirements for LDW Technical Safety Requirement 01-b:

In this case, the E2E protection protocol used to verify data transmission is shown below.



ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-b-i	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 (E2E) protection mechanism	C	E2ECalc	LDW_Torq_Req= 0 (Nm)
Software Safety Requirement 01-b-ii	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)

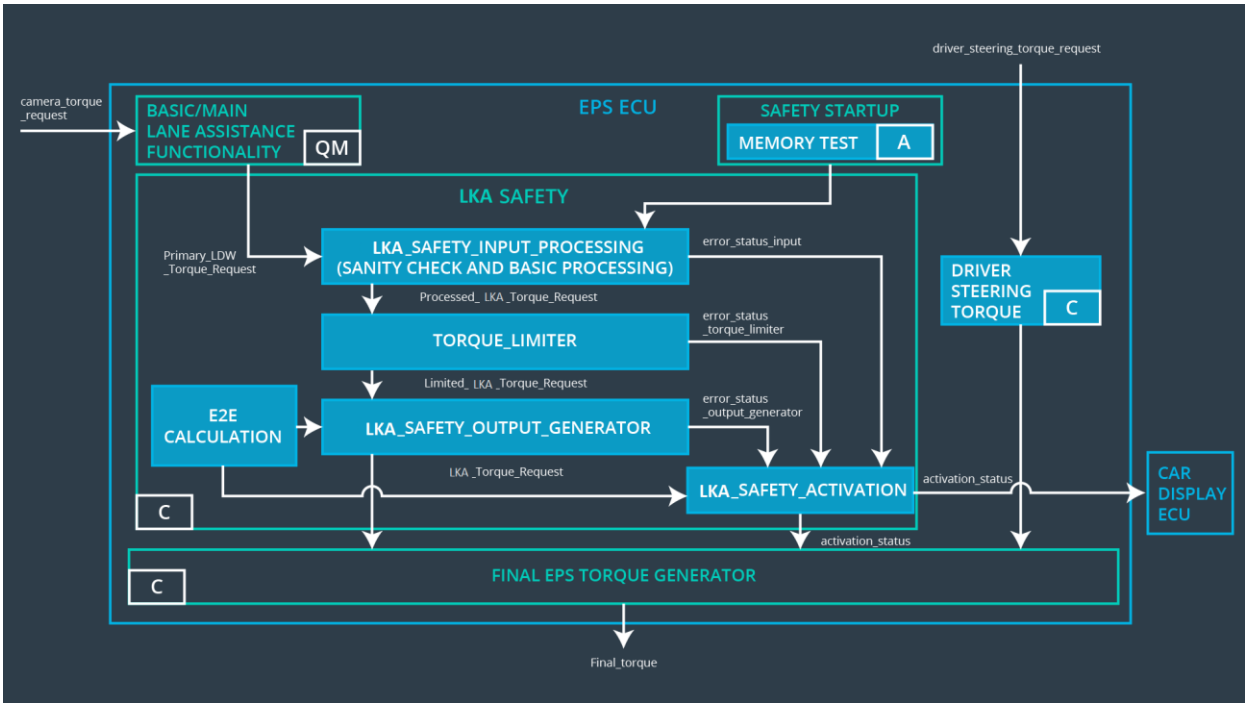
Software requirements for LDW Technical Safety Requirement 01-c:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-c-i	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-c-ii	In case the “processed_LDW_Torq_Req” signal has a amplitude and frequency greater than “Max_Torque_Ampltide_LDW” and “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-c-iii	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)

Software requirements for LDW Technical Safety Requirement 01-d:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-d-i	Each of the SW elements shal loutput 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(TORQUE_LIMITER), error_status_output_gen(LDW_SAFETY_OUTPUT_GENERATOR)	C	All	N/A
Software Safety Requirement 01-d-ii	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-d-iii	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-d-iv	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
Software Safety Requirement 01-d-v	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)
Software Safety Requirement 01-d-vi	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

For the following technical safety requirement, software requirements are identified and allocated the architecture diagram in the following manner.



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

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	C	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 .	C	50 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	C	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	C	50 ms	LKA Safety Block	Set LKA torque to zero

Software requirements for LKA Technical Safety Requirement 02-a:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-a-i	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	LKA_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 02-a-ii	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)

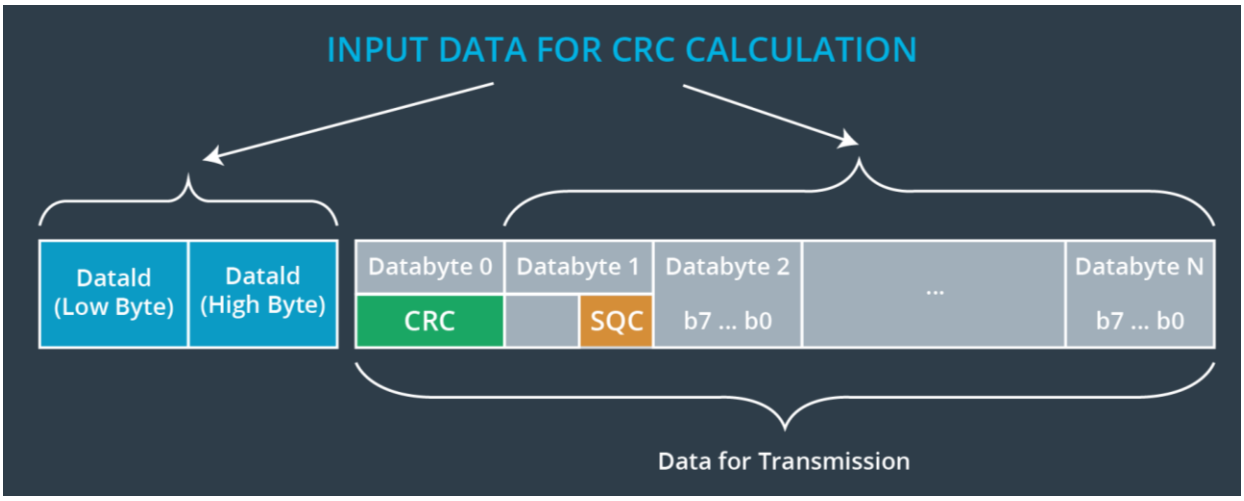
Software Safety Requirement 02-a-iii	The “limited_LKA_Torq_Req”shall be transformed into a signal “LKA_Torq_Req” whichis suitable to be transmittedoutside of the LDW Safetycomponent (LKA Safety”) to the “Final EPS Torque”component.	B	LKA_SAFETY_OUTPUT_GENERATOR	LKA_Torq_Req= 0 (Nm)

Software requirements for LKA Technical Safety Requirement 02-b:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-b-i	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 02-b-ii	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 (E.g. waking 1s test, RAM pattern test. Refer RAM and processor vendor recommendations)	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 02-b-iii	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-b-iv	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 LKATorque is set to 0	A	LKA_SAFETY_INPUT_PROCESSING	Activation_status = 0

Software requirements for LDW Technical Safety Requirement 02-c:

In this case, the E2E protection protocol used to verify data transmission is shown below.



ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-c-i	Any data to be transmitted outside of the LKA Safety component (“LKA Safety”)including "LKA_Torque_Req"and “activation_status” shall be protected by an End2End (E2E) protection mechanism	C	E2ECalc	LKA_Torq_Req= 0 (Nm)
Software Safety Requirement 02-c-ii	The E2E protection protocol shall contain and attach the control data: alive counter (SQC) and CRC to the data to be transmitted.	C	E2ECalc	LKA_Torq_Req= 0 (Nm)

Software requirements for LDW Technical Safety Requirement 02-d:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-d-i	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-d-ii	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-d-iii	The “limited_LKA_Torq_Req” shall be transformed into a signal “LKA_Torq_Req” which is suitable to be transmitted outside of the LKA Safety component (“ LKA Safety”) to the “Final EPS Torque”component.	B	LKA_SAFETY_OUTPUT_GENERATOR	LKA_Torq_Req= 0 (Nm)

Software requirements for LDW Technical Safety Requirement 02-e:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-e-i	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 (TORQUE_LIMITER),	C	All	N/A

	error_status_output_gen (LKA_SAFETY_OUTPUT_GENERATOR)			
Software Safety Requirement 02-e-ii	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)	C	LKA_SAFETY_ACTIVATION	Activation_status = 0 (LKA function deactivated)
Software Safety Requirement 02-e-iii	In case of no errors from the software elements, the status of the LKA feature shall be set to activated (“activation_status”=1)	C	LKA_SAFETY_ACTIVATION	N/A
Software Safety Requirement 02-e-iv	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	LKA_Torq_Req = 0
Software Safety Requirement 02-e-v	Once the LKA functionality has been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again.	C	LKA_SAFETY_ACTIVATION	Activation_status = 0 (LKA function deactivated)
Software Safety Requirement 02-e-vi	When the LKA function is deactivated (activation_status set to 0), the activation_status shall be sent to the car displayECU.	C	LKA_SAFETY_ACTIVATION, CarDisplay ECU	N/A

Refined Architecture Diagrams