Software Safety Requirements and Architecture
Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-06-14	1.0	Markus Isaksson	First attempt

Table of Contents

Purpose

The Software Safety Requirements and Architecture document refines the Technical Safety Concept by adding all details needed by a software engineer to develop the program. This may include variable names, signal paths, protocols and mechanisms. The granularity of the architecture is refined to describe software elements/units within components.

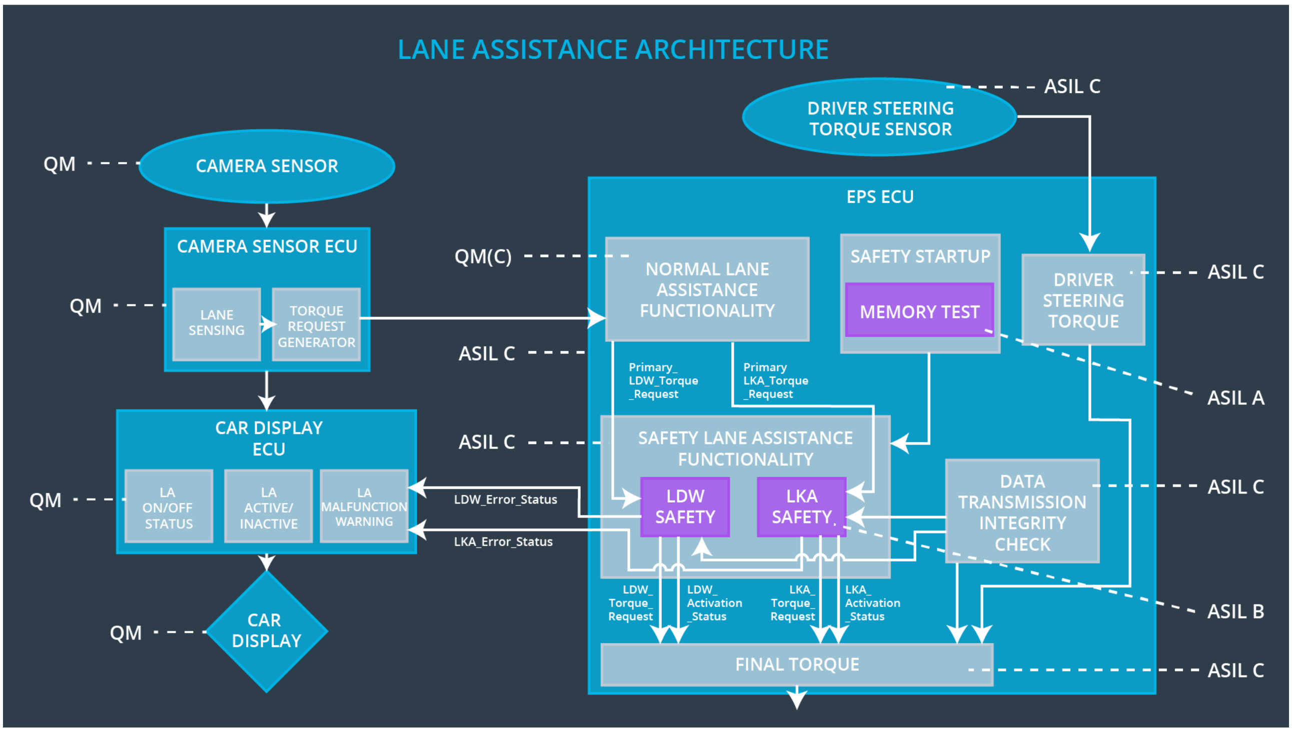
Inputs to the Software Requirements and Architecture Document

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 Torque' component is below Max_Torque_Amplitude.	C	50 ms	LDW Safety	Lane Assistance is turned off
Technical Safety Requirement 02	When a failure is detected by the 'LDW Safety' component, this shall be indicated in the LDW_Torque_Request signal.	C	50 ms	LDW Safety	Lane Assistance is turned off
Technical Safety Requirement 03	When the 'Final Torque' component receives a LDW_Torque_Request signal indicating a failure, then it shall set LA_Final_Torque to zero.	C	50 ms	Final Torque	Lane Assistance is turned off
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	Lane Assistance is turned off
Technical Safety Requirement 05	When a failure is detected by the 'LDW Safety' component,this shall be indicated in the LDW_Error_Status signal.	C	50 ms	LDW Safety	Lane Assistance is turned off
Technical Safety Requirement 06	When the 'LA Malfunction Warning' component receives a LDW_Error_Status signal indicating a failure, then it shall draw a symbol on the Car Display indicating that the LA item is turned of due to a malfunction.	QM	50 ms	LA Malfunction Warning	Lane Assistance is turned off
Technical Safety Requirement 07	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	Lane Assistance is turned off

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	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the ‘Final Torque’ component is below Max_Torque_Amplitude.	C	50 ms	LDW Safety	Lane Assistance is turned off

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State

Software Safety Requirement 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 01-02	In case the “processed_LDW_Torq_Req” signal has a value greater than “Max_Torque_Amplitude_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 01-03	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. Also see SofSafReq04-01 and SofSafReq04-02	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 02	When a failure is detected by the ‘LDW Safety’ component, this shall be indicated in the LDW_Torque_Request signal.	C	50 ms	LDW Safety	Lane Assistance is turned off

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01	The limited_LDW_Torq_Req signal shall have a boolean field Torq_Failure indicating failures.	C	TORQUE_LIMITER	N/A
Software Safety Requirement 02-02	When Torque_Limiter actively limits the “limited_LDW_Torq_Req” to 0, then the Torq_Failure shall be set to True, otherwise it shall be set to False. Also see SofSafReq01-02.	C	TORQUE_LIMITER	N/A
Software Safety Requirement 02-03	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. Also see SofSafReq04-01 and SofSafReq04-02	C	LDW_SAFETY_OUTPUT_GENERATOR	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 03	When the ‘Final Torque’ component receives a LDW_Torque_Request signal indicating a failure, then it shall set LA_Final_Torque to zero.	C	50 ms	Final Torque	Lane Assistance is turned off

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	When the ‘Final Torque’ component receives a “LDW_Torq_Req” signal where the Torq_Failure value is True, then it shall set the Final_Torque to 0 until end of power cycle.	C	FINAL_EPS_TORQUE_GENERATOR	Final_Torque set to 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	Data Transmission Integrity Check	Lane Assistance is turned off

ID	Software Safety Requirement	ASIL	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” (see SofSafReq03-02) shall be protected by an End2End(E2E) protection mechanism	C	E2ECalc	LDW_Torq_Req= 0 (Nm)
Software Safety Requirement 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)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	When a failure is detected by the ‘LDW Safety’ component,this shall be indicated in the LDW_Error_Status signal.	C	50 ms	LDW Safety	Lane Assistance is turned off

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 05-01	When Torque_Limiter actively limits the “limited_LDW_Torq_Req” to 0, then the LDW_Error_Status signal be set to “LDW_Torq_Failure”. Also see SofSafReq01-02.	C	TORQUE_LIMITER	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State

Technical Safety Requirement 06	When the ‘LA Malfunction Warning’ component receives a LDW_Error_Status signal indicating a failure, then it shall draw a symbol on the Car Display indicating that the LA item is turned of due to a malfunction.	QM	50 ms	LA Malfunction Warning	Lane Assistance is turned off

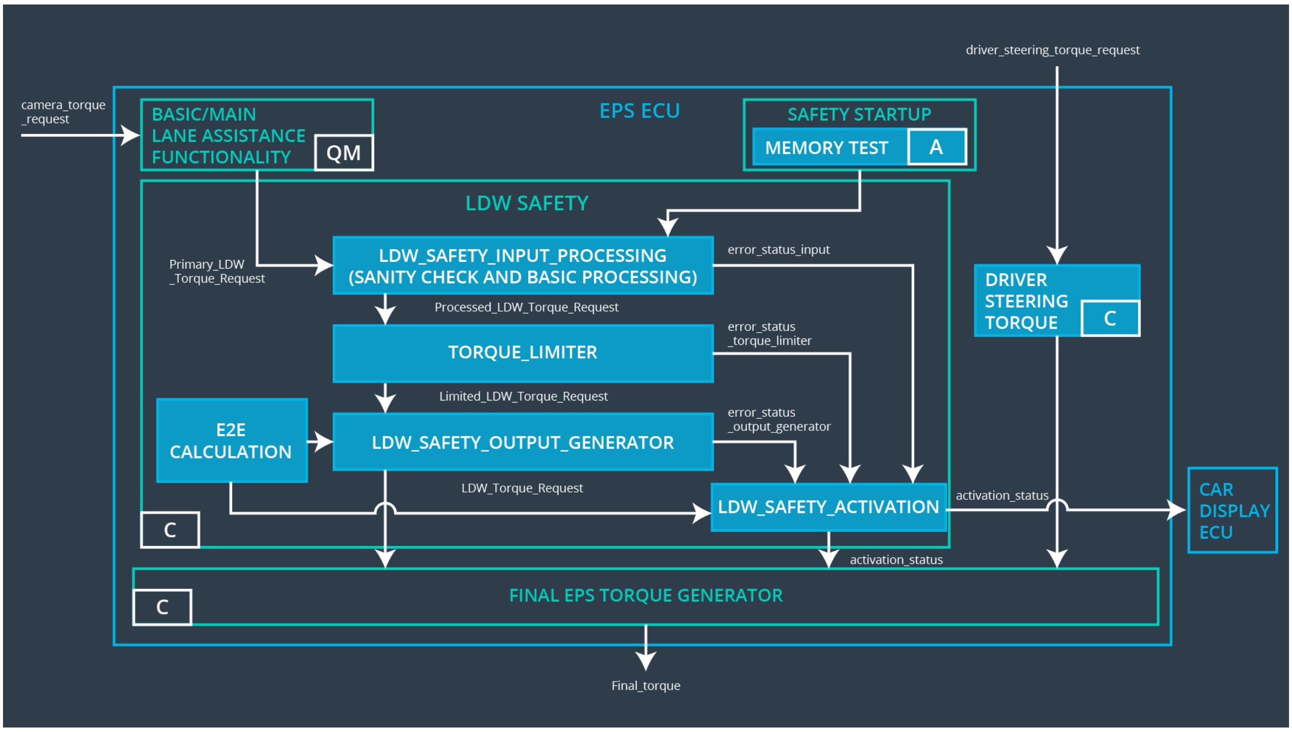
ID	**Software Safety Requirement**	**ASIL**	**Allocation Software Elements**	**Safe State**
Software Safety Requirement 06-01	When the ‘LA Malfunction Warning’ component receives a LDW_Error_Status signal having the value “LDW_Torq_Failure” or “LDW_Memory_Failure”, then it shall draw both the LA_OFF and the LA_Malfunction symbol on the display.	QM	CAR_DISPLAY_ECU - LA Malfunction Warning	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 07	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	Lane Assistance is turned off

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 07-01	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 07-02	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.walking 1s test, RAM pattern test. Refer RAM and processor vendor recommendations)	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 07-03	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 07-04	In case any fault is indicated via the “test_status” signal the INPUT_LDW_PROCESSING shall set an error on error_status_input (=1)	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0
Software Safety Requirement 07-05	When the error_status_input indicates an error, the activation status shall be set to False and the LDW_Error_Status signal set to “LDW_Memory_Failure”.		LDW_SAFETY_ACTIVATION	

Software Safety Requirement 07-06	When the ‘Final Torque’ component receives a activation status with value False, then it shall set the Final_Torque to 0 until end of power cycle.	C	FINAL_EPS_TORQUE_GENERATOR	Final_Torque set to 0

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

This figure is not completely accurate to the final architecture (but considered good enough for this exercise). In particular the error handling is done differently, except for the memory test.