Software Safety Requirements and Architecture

Lane Assistance

Document Version: 1.0

Version 1.0, Released on 2018-04-29

Document history

Date	Version	Editor	Description
04/29/2018	1.0	Ninad Ghike	Initial Creation

Table of Contents

Purpose

The purpose of the Software Safety Requirements and Architecture Lane Assistance is to define software safety requirements

Inputs to the Software Requirements and Architecture Document

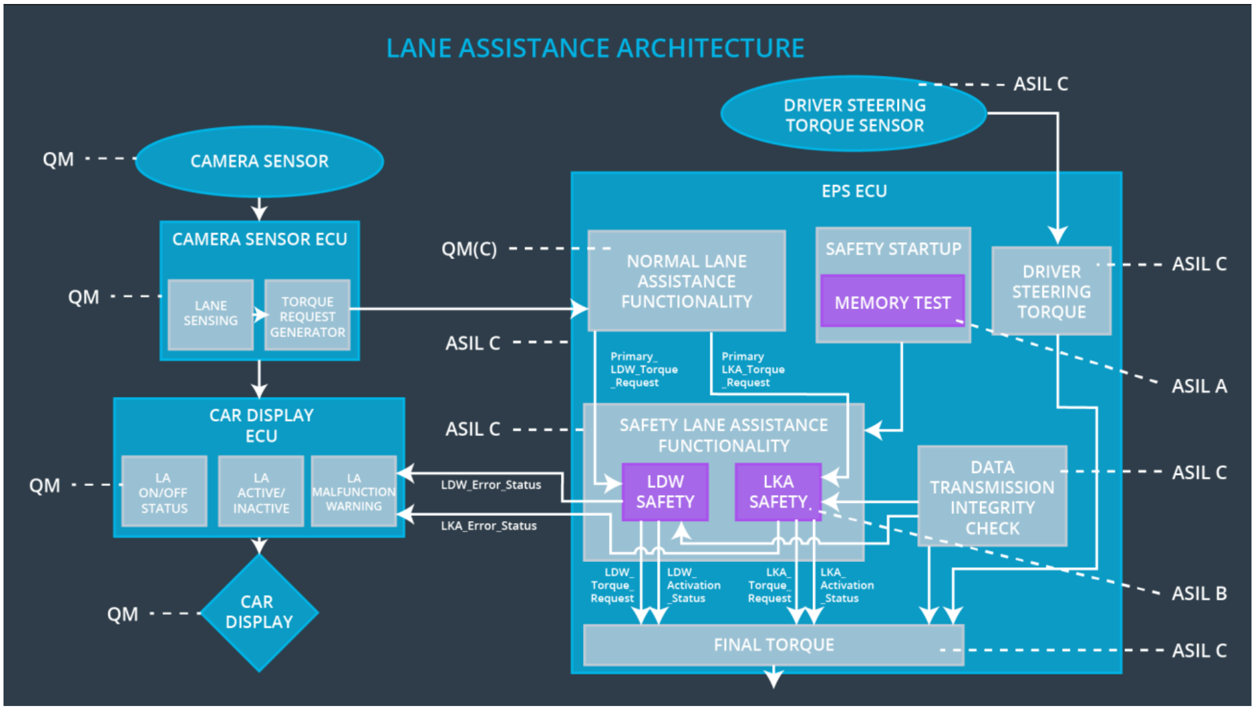
Technical safety requirements

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	50 msec	LDW Safety Functionality	OFF
Technical Safety Requirement 02	The 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light as soon as the LDW function deactivates the LDW feature.	C	50 msec	LDW Safety Functionality	OFF
Technical Safety Requirement 03	The LDW function shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero as soon as a failure is detected.	C	50 msec	LDW Safety Functionality	OFF
Technical Safety Requirement 04	The system shall check for the timeouts of ‘LDW_Torque_Request’ Signal	C	50 msec	Data Transmission integrity check	OFF

Technical Safety Requirement 05	The system shall perform memory check of the EPS ECU at bootup to look for memory related faults.	A	Ignition Cycle	Safety Startup	OFF

Refined Architecture Diagram from the Technical Safety Concept



Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

ID	Technical Safety Requirement	A S I L	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	50 msec	LDW Safety Functionality	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_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	The “limited_LDW_Torq_Req”shall be transformed into a signal	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	The 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light as soon as the LDW function deactivates the LDW feature.	C	50 msec	LDW Safety Functionality	OFF

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01	Each of the software 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 (TORQUE_LIMITER), error_status_output_gen (LDW_SAFETY_OUTPUT_GENERATOR)	C	All	N/A
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 the LDW feature (“activation_status”=0)	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)
Software Safety Requirement 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	In case an error is detected by any of the software elements, it	C	All	LDW_Torq_Req = 0

Requirement 02-04	shall set the value of its corresponding torque to 0 so			
Software Safety Requirement 02-01	Each of the software 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 (TORQUE_LIMITER), error_status_output_gen (LDW_SAFETY_OUTPUT_GENERATOR)	C	All	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 03	The LDW function shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero as soon as a failure is detected.	C	50 msec	LDW Safety Functionality	OFF

ID	Software Safety Requirement	ASIL	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 Display ECU	C	LDW_SAFETY_ACTIVATION, CarDisplay ECU	N/A

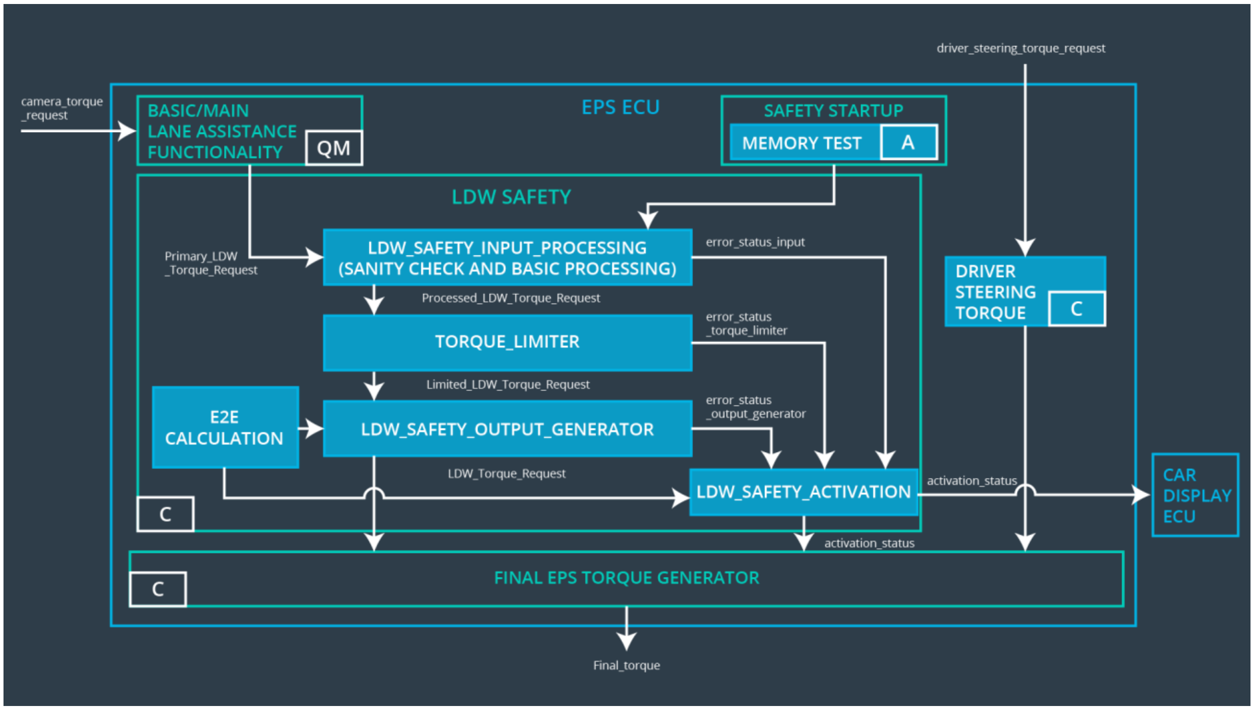
ID	Technical Safety Requirement	A S I L	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 04	The system shall check for the timeouts of ‘LDW_Torque_Request’ Signal	C	50 msec	Data Transmission integrity check	OFF

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” (see SofSafReq 02-02) shall be protected by an E2E protection mechanism	C	E2E Calculation	LDW_Torq_Req= 0
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	E2E Calculation	LDW_Torq_Req= 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	The system shall perform memory check of the EPS ECU at bootup to look for memory related faults.	A	Ignition Cycle	Safety Startup	OFF

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 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 Safety Requirement 05-02	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 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 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 LDW Torque is set to 0	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 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