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
06/13/2018	1.0	Swapnil More	First Draft
06/15/2018	1.1	Swapnil More	Updates to First Draft

Table of Contents

Purpose

This document identifies the new requirements for the software components at a component level to identify potential problems on software design and architecture that could lead to a violation of safety goals. These requirements are more detail oriented than the technical safety concept requirements.

Inputs to the Software Requirements and Architecture Document

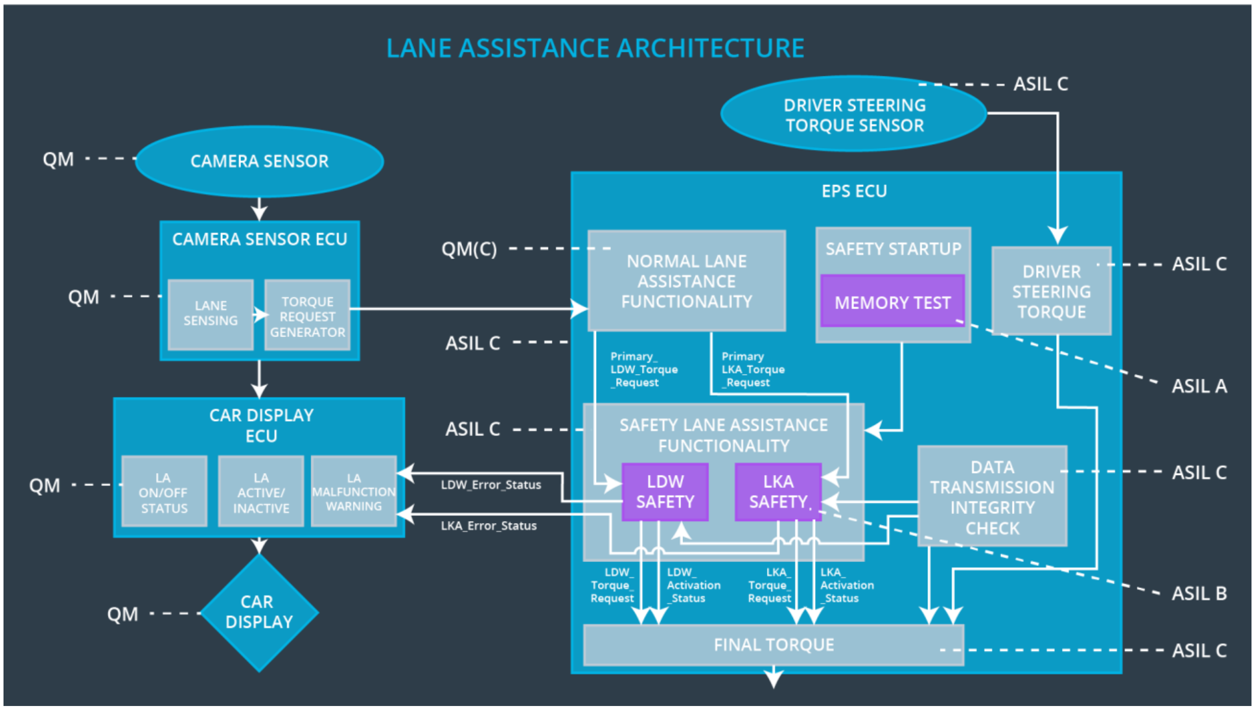
Technical safety requirements

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 01-01-01	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	Lane Departure Warning Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 01-01-02	When the LDW is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	Lane Departure Warning Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 01-01-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	Lane Departure Warning Torque Request Amplitude shall be set to zero.
Technical Safety Requirement	The validity and integrity of the data transmission for	C	50 ms	Data Transmission Integrity	Lane Departure Warning

01-01-04	‘LDW_Torque_Request’ signal shall be ensured.			Check	Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any memory problems	A	Ignition cycle	Memory Test	Lane Departure Warning Torque Request Amplitude shall be set 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	Lane Departure Warning Torque Request Amplitude shall be set 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_SAGETY_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_Amplitude_LDW' (maximum allowed safe torque), the torque signal 'limited_LDW_Torq_Req' shall be set to zero, else 'limited_LDW_Torq_Req' shall	C	TORQUE_LIMITER	'limited_LDW_Torq_Req' = 0 (Nm=Newton-meter)

	take the value of ‘processed_LDW_Torq_Req’			
Software Safety Requirement 01-01-01-03	The ‘limited_LDW_Torq_Req’ shall be transformed into a signal ‘LDW_Torq_Req’ which is suitable to be transmitted outside 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	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-02	When the LDW is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	Lane Departure Warning Torque Request Amplitude shall be set to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-02-01	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 01-01-02-02	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 01-01-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	Lane Departure Warning Torque Request Amplitude shall be set to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-03-01	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(TORQUE_LIMITER), error_status_output_gen(LDW_SAFETY_OUTPUT_GENERATOR)	C	All	N/A
Software Safety Requirement 01-01-03-02	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 01-01-03-03	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	C	LDW_SAFETY_ACTIVATION	N/A

	(“activation_status”=0)			
Software Safety Requirement 01-01-03-04	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
Software Safety Requirement 01-01-03-05	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	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	Lane Departure Warning Torque Request Amplitude shall be set to zero.

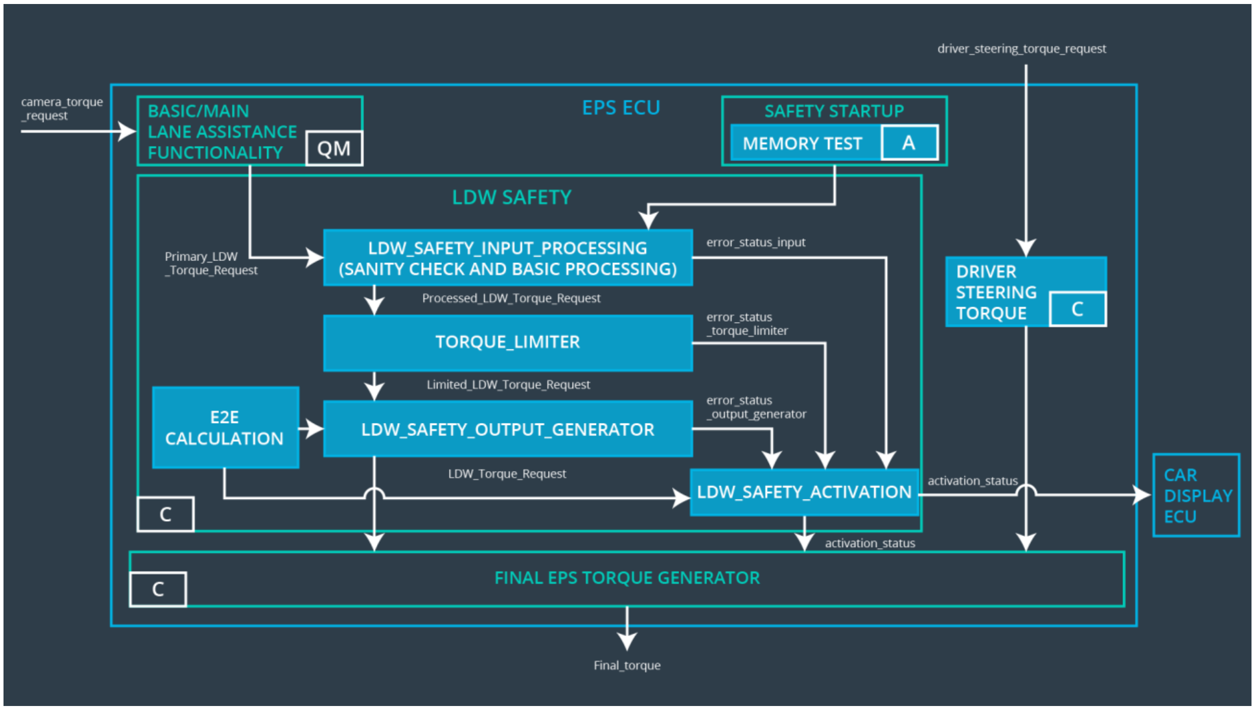
ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-04-01	When the LDW function is deactivated (activation_status set to 0), the activation_status shall be sent to the car displayECU.	C	LDW_SAFETY_ACTIVATION, CarDisplay ECU	N/A

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 startup of the EPS ECU to check for any memory problems	A	Ignition cycle	Memory Test	Lane Departure Warning Torque Request Amplitude shall be set 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 content corruption.	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 01-01-05-02	Standard RAM test 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 to RAM and processor vendor recommendations)	A	MEMORYTEST	Activation_status = 0
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 the	A	LDW_SFETY_INPUT_PROCESSING	Activation_status = 0

	error_status_input(=1) so that the Lane Departure Warning functionality is deactivated and the LDW_Torque_Req is set to zero.			

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