



Software Safety Requirements and Architecture

Lane Assistance

Document Version: 1.0
Released on 2018-06-21



Document history

Date	Version	Editor	Description
21-Jun-2018	1.0	Prathmesh Dali	Final Submission

Table of Contents

[Document history](#)

[Table of Contents](#)

[Purpose](#)

[Inputs to the Software Requirements and Architecture Document](#)

[Technical safety requirements](#)

[Refined Architecture Diagram from the Technical Safety Concept](#)

[Software Requirements](#)

[Refined Architecture Diagram](#)

Purpose

This document captures the details of software requirements and architecture which are derived from technical safety documentation. These requirements will be then analyzed and implemented by software engineers which will help in reducing the problems with software design which could further lead to safety hazards.

Inputs to the Software Requirements and Architecture Document

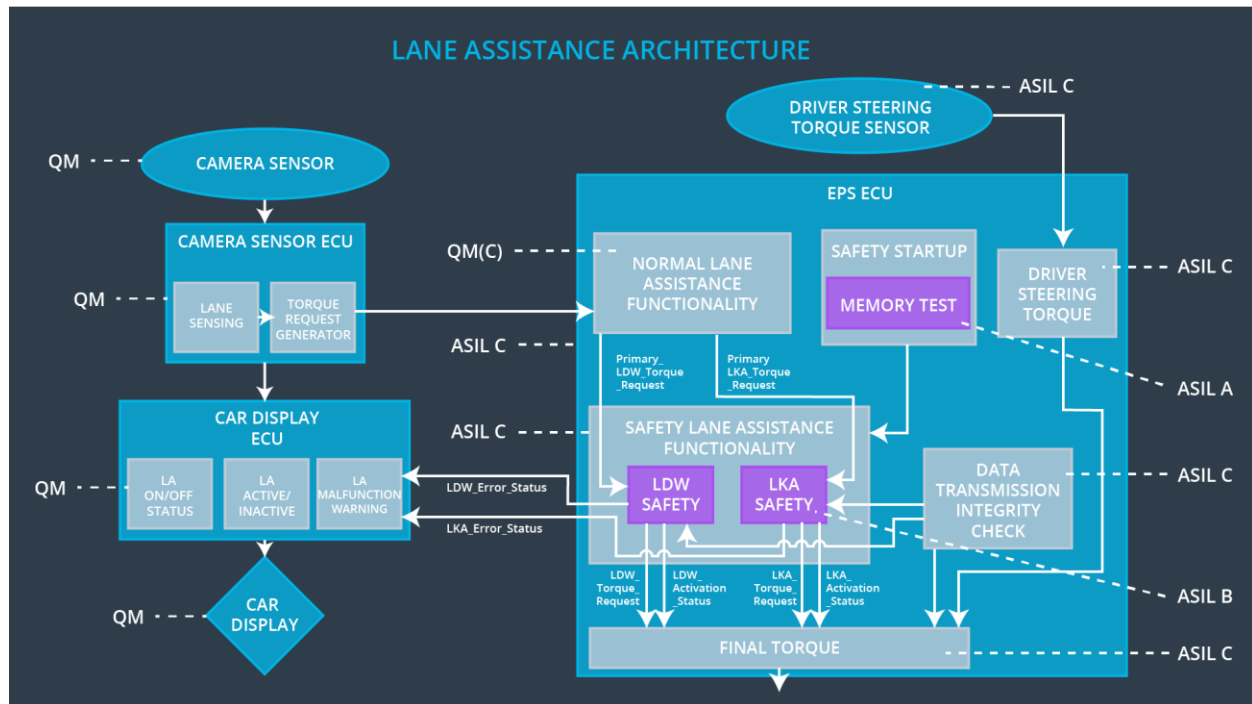
Technical safety requirements

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 Lane Departure Warning safety component shall ensure that the amplitude of the 'LDW_Torque_Request' which is sent to the 'Final electronic power steering Torque' component is less than 'Max_Torque_Amplitude'.	C	50 ms	Lane Departure Warning safety block	'LDW_Torque_Request' shall be set to zero
Technical Safety Requirement 02	As soon as the Lane Departure Warning function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display Electronic Car Unit to turn on a warning light.	C	50 ms	Lane Departure Warning safety block	'LDW_Torque_Request' shall be set to zero
Technical Safety Requirement 03	As soon as the failure is detected by the Lane Departure Warning function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	50 ms	Lane Departure Warning safety block	'LDW_Torque_Request' shall be set to zero
Technical Safety Requirement 04	The integrity and validity of the transmission of data for 'LDW_Torque_Request' signal shall be ensured.	A	50 ms	Data Transmission Integrity Check	'LDW_Torque_Request' shall be set to zero

Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	50 ms	Memory Check	'LDW_Torque_Request 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	A S I L	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The Lane Departure Warning safety component shall ensure that the amplitude of the LDW_Torque_Request which is sent to the Final Electronic Power Steering Torque component is less than Max_Torque_Amplitude	C	50 ms	Lane Departure Warning Safety	LDW torque output shall be set to zero

ID	Software Safety Requirement	A S I L	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 LAF functionality" SW Component. Signal "processed_LDW_Torq_Req" shall be generated at the end of the processing.	C	LDW_SAFETY_INPUT_P ROCESSING	N/A
Software Safety Requirement 01-02	In case the "processed_LDW_Torq_Req" signal has a value larger than "Max_Torque_Amplitude_LDW" (maximum allowed safe torque), the torque signal	C	TORQUE_LIMITER	"limited_LDW_T orq_Req" = 0(Nm=Newtonm eter)

	“limited_LDW_Torq_Req” shall be set to 0, else “limited_LDW_Torq_Req” shall take the value of “processed_LDW_Torq_Req”.			
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 Lane Departure Warning Safety component (“LDW Safety”) to the “Final EPS Torque” component. Also see SofSafReq02-01 and SofSafReq02-02			LDW_Torq_Req = 0 (Nm)

ID	Technical Safety Requirement	A S I L	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02	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	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 02-01	Any data which is to be transmitted outside of the Lane Departure Warning Safety component (“LDW Safety”) including “LDW_Torque_Req” and “activation_status” (see SofSafReq03-02) shall be protected by an End2End protection mechanism	C	E2ECalc	LDW_Torq_Req = 0 (Nm)
Software Safety	The End2End protection protocol shall contain and attach the	C	E2ECalc	LDW_Torq_Req

Requirement 02-02	control data: alive counter (SQC) and CRC to the data to be transmitted.			q= 0 (Nm)
-------------------	--	--	--	-----------

ID	Technical Safety Requirement	A S I L	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 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	LDW_torque_output=0

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	Each of the elements of SW 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 03-02	A software element shall evaluate the error status of all the other software elements and in case any one of them indicates an error, it shall deactivate the Lane Departure Warning feature ("activation_status"=0)	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)
Software Safety Requirement	In case of no errors from the software elements, the status of the LDW feature shall be	C	LDW_SAFETY_ACTIVATION	N/A

03-03	activated ("activation_status"=1)			
Software Safety Requirement 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 03-05	Once the Lane Departure Warning 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 04	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	LDW_Torque_Output=0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	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 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Memory Test	LDW_torqu _output = 0

ID	Software Safety Requirement	A S I L	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	MEMORYTES T	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	MEMORYTES T	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	MEMORYTES T	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 LDWTorque is set to 0	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

Refined Architecture Diagram

