Software Safety Requirements and Architecture

Lane Assistance

Document history

Date	Version	Editor	Description
28th May 29, 2018	1.0	Anant Yash Pande	Initial document

Table of Contents

Purpose

This document describes the new requirements for component-level software to identify potential software design and architecture issues that could lead to a breach of safety goals. The safety requirements must be developed taking into account the whole vehicle, as otherwise potential hazards could be overlooked.
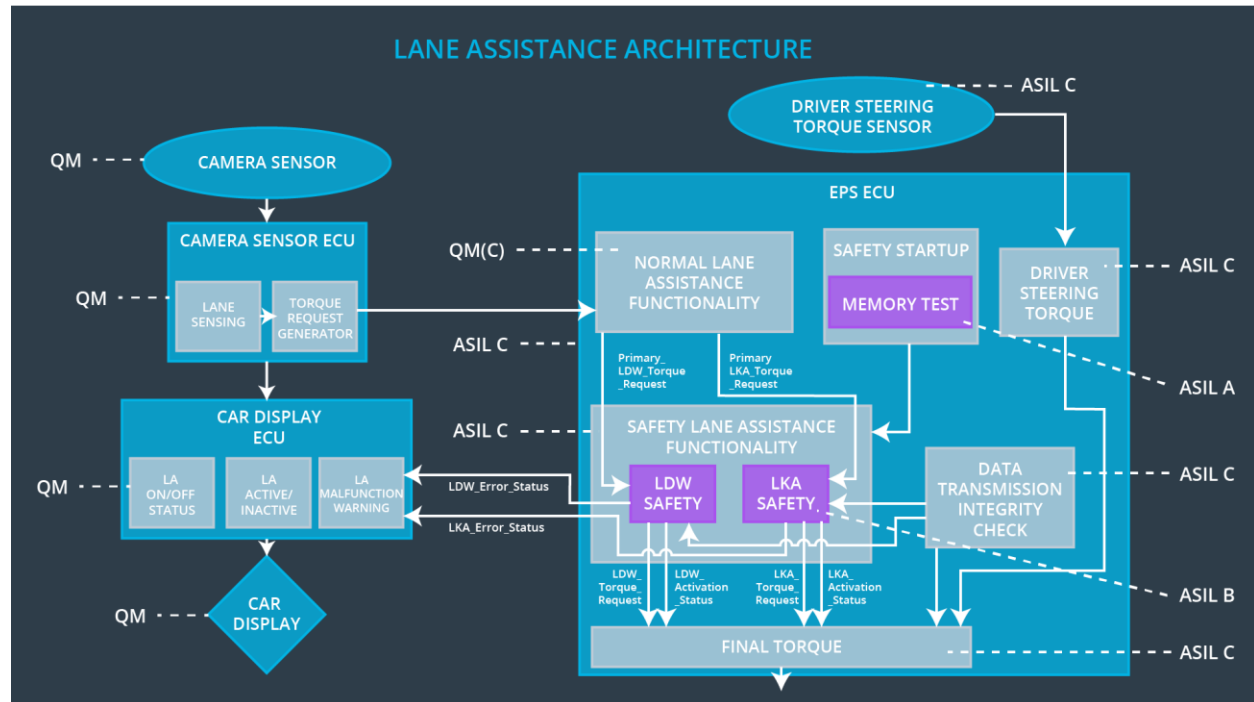
Inputs to the Software Requirements and Architecture Document

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 ms	LDW safety block	LDW_Torque _Output is set to zero
Technical Safety Requirement 02	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 block	LDW_Torque _Output is 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	Ignition cycle	Memory Test	LDW_Torque _Output is 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	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 block	LDW_Torque_Output is set to zero

ID	Software Safety Requirement	ASI	Allocation Software Elements	Safe State

		L		
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 LA 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 greater than "Max_Torque_Ampltide_LDW" (maximum allowed safe torque), the torque signal "limited_LDW_Torq_Req" shall be set to 0, and else "limited_LDW_Torq_Req" shall take the value of "processed_LDW_Torq_Req".	C	TORQUE_LIMITER	"limited_LDW_T orq_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 SofSafReq02-01 and SofSafReq02-02	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	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	ASI	Allocation Software Elements		Safe State

		L		
Software Safety Requirement 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 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 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 is set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 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_PROCESSIN G), error_status_torque_limiter (TORQUE_LIMITER), error_status_output_gen (LDW_SAFETY_OUTPUT_GE NERATOR)	C	All	N/A
Software Safety	A software element shall evaluate the error status of all	C	LDW_SAFETY _ACTIVATION	Activation_status = 0 (LDW function

ID				
Requirement 03-02	the other software elements and in case any 1 of them indicates an error, it shall deactivate the LDW feature ("activation_status"=0)			deactivated)
Software Safety Requirement 03-03	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

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 is set to zero

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, Car Display ECU	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Memory Test	LDW torque output is set to zero

ID	Software Safety Requirement	ASIL	Allocation	Safe State

		S I L	Software Elements	
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	MEMORY TEST	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	MEMORY TEST	Activation_status = 0

Refined Architecture Diagram