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
2/28/2018	1.0	Mark	First attempt while following along in classs

Table of Contents

Purpose

This document helps to ensure we have taken into account all vehicle safety requirements at the hardware and software level of the V-diagram from ISO-26262.
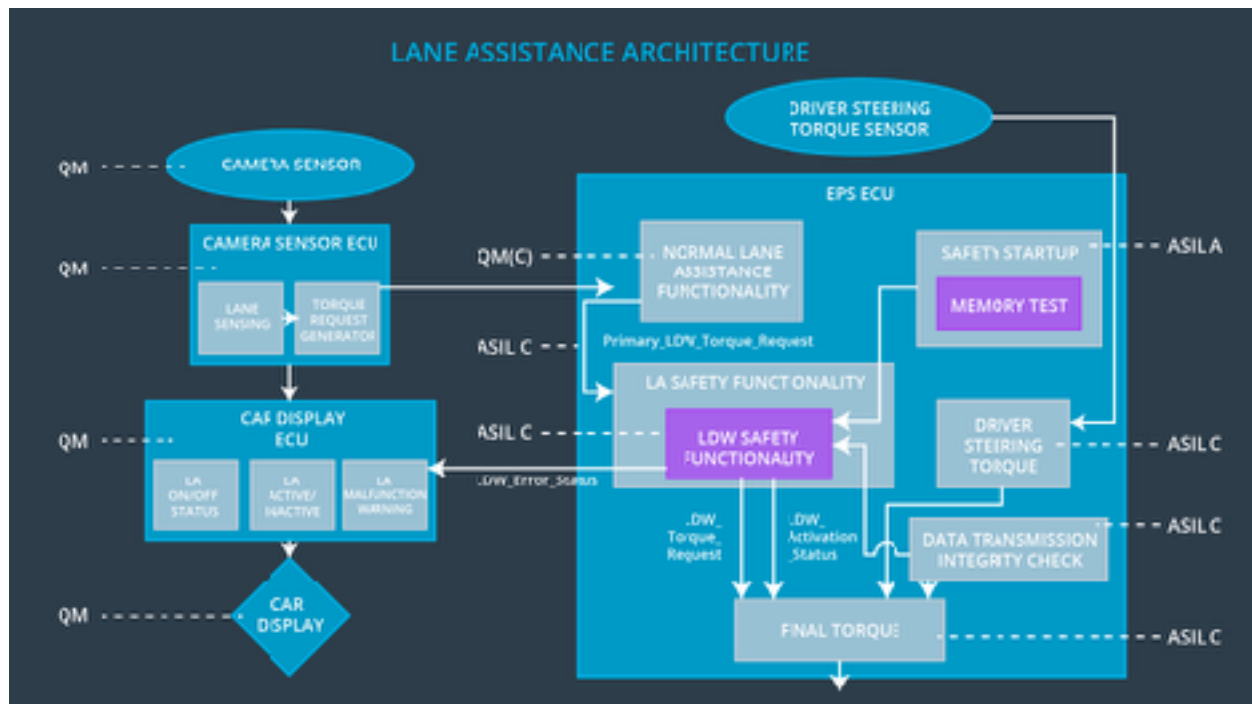
Inputs to the Software Requirements and Architecture Document

Technical safety requirements

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

Technical Safety Req. ID	Technical Safety Requirement	ASIL	FTTI	Architecture Allocation	Safe State
01	The LDW safety component shall ensure that the amplitude of the 'LDW_Torque_Request' sent to the 'Final EPS Torque' component is below 'Max_Torque_Amplitude'.	C	50 ms	LDW Safety block	LDW_Torque_Request Amplitude shall be set to zero
02	As soon as LDW deactivates the 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_Request Amplitude shall be set to zero
03	As soon as a failure is detected by the LDW, it shall deactivate the feature and the 'LDW_Torque_Request' shall be set to zero	C	50 ms	LDW Safety block	LDW_Torque_Request Amplitude shall be set to zero
04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50 ms	Data Transmission Integrity Check	LDW_Torque_Request Amplitude shall be set to zero
05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Safety Startup Memory Test	LDW_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:

Technical Safety Req. ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
01	The LDW safety component shall ensure that the amplitude of the 'LDW_Torque_Request' sent to the 'Final EPS Torque' component is below 'Max_Torque_Amplitude'.	C	50 ms	LDW Safety block	LDW_Torque_ Request Amplitude shall be set to zero

Software Safety Req. ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
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
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
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)

Technical Safety Req. ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
02	As soon as LDW deactivates the 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_Request Amplitude shall be set to zero

Software Safety Req. ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
02-01	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

Technical Safety Req. ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
03	As soon as a failure is detected by the LDW, it shall deactivate the feature and the 'LDW_Torque_Request' shall be set to zero	C	50 ms	LDW Safety block	LDW_Torque_Request Amplitude shall be set to zero

Software Safety Req. ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
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
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)
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
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
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)

Technical Safety Req. ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50 ms	Data Transmission Integrity Check	LDW_Torque_Request Amplitude shall be set to zero

Software Safety Req. ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
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
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

Technical Safety Req. ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Safety Startup Memory Test	LDW_Torque _Request Amplitude shall be set to zero

Software Safety Req. ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
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
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
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
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_PROCE SSING	Activation_ status = 0

Refined Architecture Diagram