Elektrobit

UDACITY

Software Safety Requirements and Architecture

Lane Assistance

Document Version: 3.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-03-13	1.0	Abhishek Mantha	Document initialization
2018-03-13	2.0	Abhishek Mantha	Revising for Final Submission
2018-03-14	3.0	Abhishek Mantha	Final Submission

Table of Contents

Purpose

The purpose of the Software Requirements and Architecture Document is to develop requirements and metrics which the item can be verified that will ensure its functional safety.

Inputs to the Software Requirements and Architecture Document

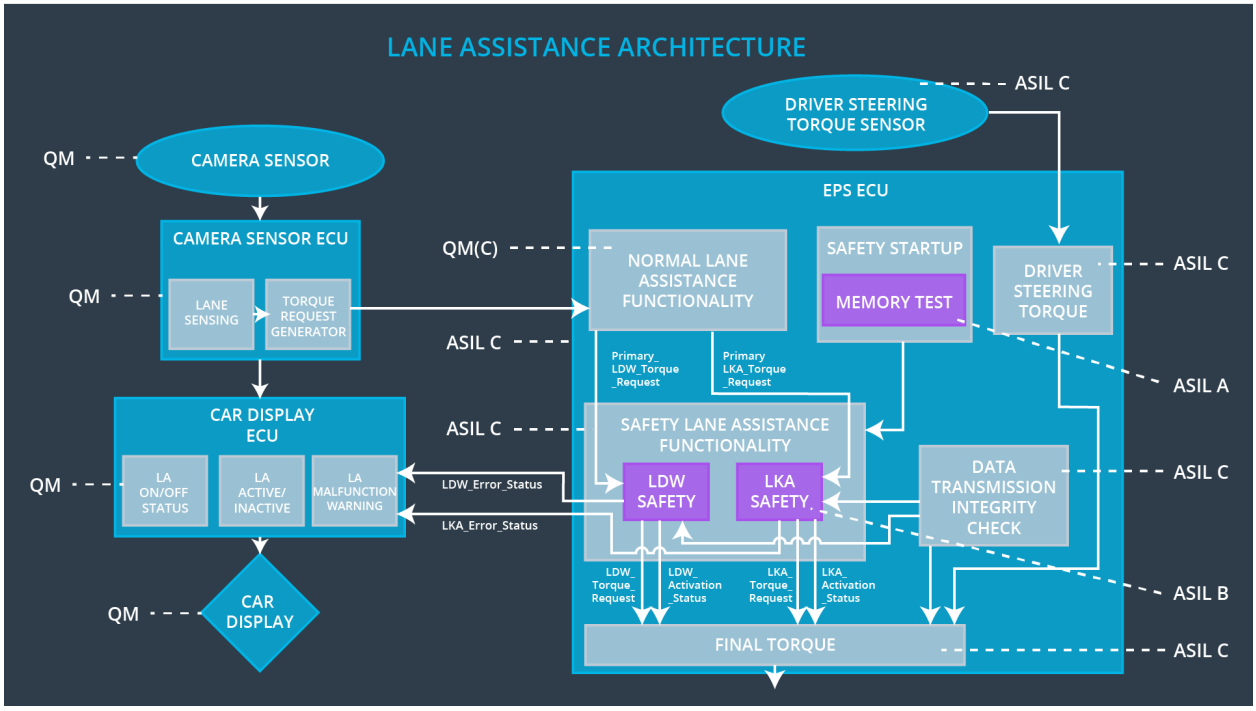
Technical safety requirements

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

ID	Technical Safety Requirement	A S	Fault Tolerant	Architecture Allocation	Safe State

		IL	Time Interval		
Technical Safety Requirement 01	LDW safety block shall ensure that amplitude of ‘LDW_Torque_Request’ sent to EPS ‘Final Torque’ component is below ‘Max_Torque_Amplitude’.	C	50 ms	LDW Safety Functionality Block	‘LDW_Torque_Request’ shall be set to 0.
Technical Safety Requirement 02	As soon as LDW function deactivates LDW feature, the 'LDW Safety' software block shall send ‘LDW_Error_Status’ to car display ECU to turn on warning light.	C	50 ms	LDW Safety Functionality Block	‘LDW_Torque_Request’ shall be set to 0.
Technical Safety Requirement 03	As soon as failure is detected by LDW function, it shall deactivate LDW feature and 'LDW_Torque_Request' shall be set to 0.	C	50 ms	LDW Safety Functionality Block	‘LDW_Torque_Request’ shall be set to 0.
Technical Safety Requirement 04	Validity and integrity of data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check Component	‘LDW_Torque_Request’ shall be set to 0.
Technical Safety Requirement 05	Memory test shall be conducted at start up of EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup Component	‘LDW_Torque_Request’ shall be set to 0.

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	Architecture Allocation	Safe State
Technical Safety Requirement 01	LDW safety block shall ensure that amplitude of 'LDW_Torque_Request' sent to EPS 'Final Torque' component is below 'Max_Torque_Amplitude'.	C	50 ms	LDW Safety Functionality Block	'LDW_Torque_Request' shall be set to 0.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software	Input signal	C	LDW_SAFETY_INPUT_P	N/A

Safety Requirement 01-01	“Primary_LDW_Torq_Req” shall be read and pre-processed to determine torque request coming from “Basic/Main LAFunctionality” SW Component. Signal “processed_LDW_Torq_Req” shall be generated at end of processing.		ROCESSING	
Software Safety Requirement 01-02	In case “processed_LDW_Torq_Req” signal has a value greater than “Max_Torque_Amplitude_LDW” (maximum allowed safe torque), torque signal “limited_LDW_Torq_Req” shall be set to 0, else “limited_LDW_Torq_Req” shall take value of “processed_LDW_Torq_Req”.	C	TORQUE_LIMITER	“limited_LDW_Torq_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 “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	Architecture Allocation	Safe State
Technical Safety Requirement 02	As soon as LDW function deactivates LDW feature, the 'LDW Safety' software block shall send ‘LDW_Error_Status’ to car display ECU to turn on warning light.	C	50 ms	LDW Safety Functionality Block	‘LDW_Torque_Request’ shall be set to 0.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 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, Car Display ECU	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 03	As soon as failure is detected by LDW function, it shall deactivate LDW feature and 'LDW_Torque_Request' shall be set to 0.	C	50 ms	LDW Safety Functionality Block	'LDW_Torque_Request' shall be set to 0.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	Each of SW elements shall output a signal to indicate any error which is detected by 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	Software element shall evaluate error status of all 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 03-03	In case of no errors from software elements, status of LDW feature shall be set to activated (“activation_status”=1)	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement 03-04	In case an error is detected by any of software elements, it shall set 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 LDW functionality has been deactivated, it shall stay deactivated till 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	Architecture Allocation	Safe State
Technical Safety Requirement 04	Validity and integrity of data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check Component	‘LDW_Torque_Request’ shall be set to 0.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	Any data to be transmitted outside of 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 04-02	E2E protection protocol shall contain and attach control data: alive counter (SQC) and CRC to data to be transmitted.	C	E2ECalc	LDW_Torq_Req= 0 (Nm)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 05	Memory test shall be conducted at start up of EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup Component	'LDW_Torque_Request' shall be set to 0.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 05-01	CRC verification check over software code in Flash memory shall be done every time 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 data bus, address bus and device integrity shall be done every time 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	Test result of RAM or Flash memory shall be indicated to LDW_Safety component via "test_status" signal	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 05-04	In case any fault is indicated via "test_status" signal INPUT_LDW_PROCESSING shall set an error on error_status_input (=1) so that LDW functionality is deactivated and LDWTorque is set to 0	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

Refined Architecture Diagram