Elektrobit

UDACITY

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
23rd May, 2019	1.0	Microsoft Word	Initial Version of Software Requirements and Architecture

Table of Contents

Purpose

The Software Safety Requirements and Architecture document outlines the safety requirements from the software point of view and allocates these software safety requirements to the overall software system architecture.

Inputs to the Software Requirements and Architecture Document

[Instructions:

REQUIRED:
You are only required to develop this document for the LDW (lane departure warning) amplitude malfunction. So here, provide the technical safety requirements for the LDW amplitude malfunction as well as the refined system architecture diagram from the technical safety concept.

OPTIONAL:
Expand this document to include software safety requirements for the LDW frequency malfunction as well. Go even further and document software safety requirements for the Lane Keeping Assistance (LKA) function as well.
]

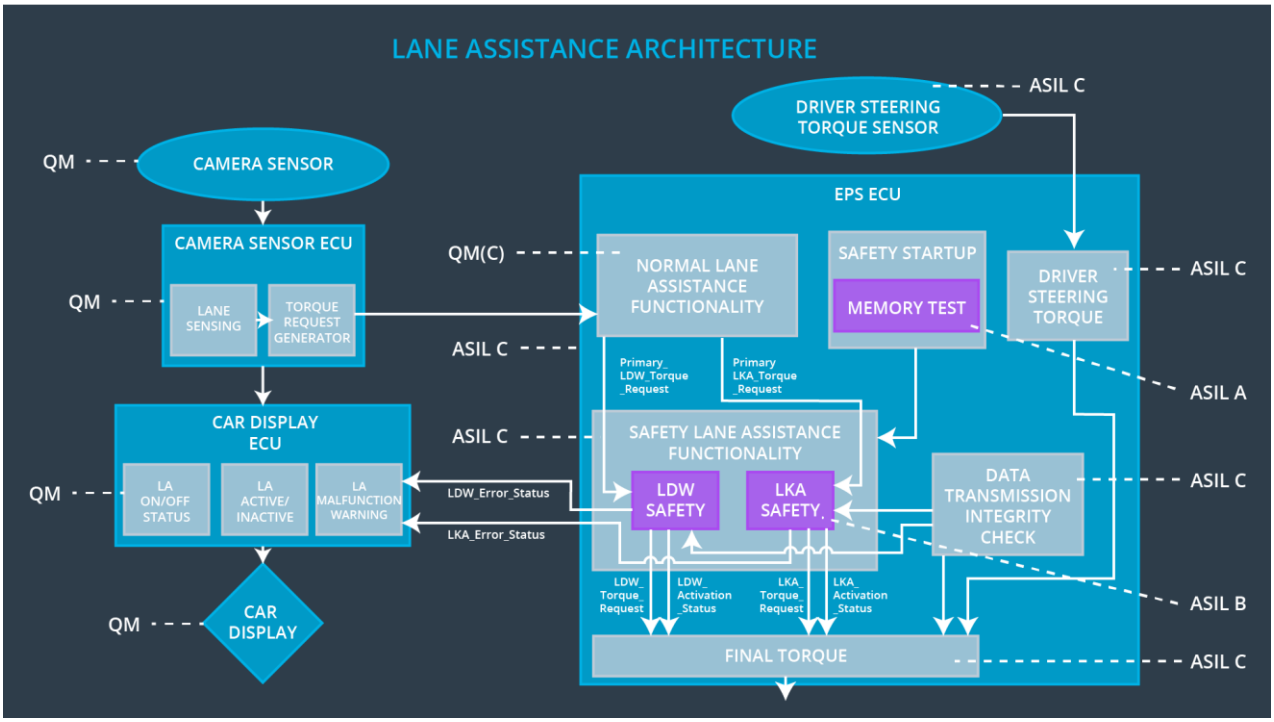
Technical safety requirements

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	LDW safety component shall ensure that the amplitude of the *LDW_torque_request* sent to the *Final Electronic*	C	50ms	LDW Safety Block	
	Power Steering Torque				
	component is below				
	Max_torque_amplitude				
					The lane departure warning torque request amplitude shall be set to zero
Technical Safety Requirement 02	Validity and Integrity of the data transmission for the *LDW_Torque_Request* signal shall be ensured	C	50ms	Data Transmission Integrity Check	
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the	C	50ms	LDW Safety Block	
	LDW_Torque_Request shall be set to zero.				

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	50ms	LDW Safety Block	The lane departure warning torque request amplitude shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at the startup of EPS ECU to check for any faults in memory.	A	Ignition cycle	Separate External block with Memory test code	

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	50ms	LDW Safety Block	The 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	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_PROCESSING	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, else“limited_LDW_Torq_Req” shall take the value of “processed_LDW_Torq_Req”	C	TORQUE_LIMITER	“limited_LDW_Torq_Req” = 0(Nm=Newton-meter)
Software Safety Requirement	The “limited_LDW_Torq_Req” shall be transformed into a signal “LDW_Torq_Req” which is	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

01-03	suitable to be transmitted outside of the LDW Safety component (“LDW Safety”) to the “Final EPS Torque” component. Also see SofSafReq02-01 andSofSafReq02-02			

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	50ms	Data Transmission Integrity Check	The lane departure warning torque request amplitude shall be set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
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” (seeSofSafReq03-02) 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	C	50 ms	LDW Safety	LDW torque output is set to zero
	be set to zero				

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software	Each of the SW elements shal l	C	All	N/A
Safety	output a signal to indicate any			
Requirement	error which is detected by the			
03-01	element. Error signal =			
	error_status_input(LDW_SAFET			
	Y_INPUT_PROCESSING),			
	error_status_torque_limiter(TOR			
	QUE_LIMITER),			
	error_status_output_gen(LDW_			
	SAFETY_OUTPUT_GENERAT			
	OR)			
Software	A software element shall	C	LDW_SAFETY	Activation_status = 0
Safety	evaluate the error status of all		_ACTIVATION	(LDW function
Requirement	the other software elements and			deactivated)
03-02	in case any 1 of them indicates			
	an error, it shall deactivate			
	theLDW			
	feature(“activation_status”=0)			
Software	In case of no errors from the	C	LDW_SAFETY	N/A
Safety	software elements, the status of		_ACTIVATION	
Requirement	the LDW feature shall be set to			
03-03	activated (“activation_status”=1)			
Software Safety	In case an error is detected by any of the software elements, it	C	All	LDW_Torq_Req = 0

Requirement 03-04	shall set the value of its corresponding torque to 0 so that “LDW_Torq_Req” is set to 0			
Software Safety Requirement 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 04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display	C	50ms	LDW Safety	LDW torque output is set to zero
	ECU to turn on a warning light				

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software	When the LDW function is	C	LDW_SAFET	N/A
Safety	deactivated (activation_status		Y_ACTIVATIO	
Requirement	set to 0), the activation_status		N, Car Display	
04-01	shall be sent to the car display		ECU	
	ECU			

ID	Technical Safety Requirement	ASIL	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	50ms	Ignition Cycle	LDW torque output is set to zero

ID	Software Safety Requirement	ASIL	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	MEMORYTEST	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	MEMORYTEST	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	MEMORYTEST	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	MEMORYTEST	Activation_status = 0

Refined Architecture Diagram