Elektrobit

UDACITY

Software Safety Requirements and Architecture Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
14.09.2017	1.0	Sergei Dmitriev	Initial version

Abbreviation List

N	Abbreviation	Definition
1.	ASIL	Automotive Safety Integrity Level
2.	CRC	Cyclic Redundancy Check
3.	E2E	End to End
4.	ECU	Electronic Control Unit
5.	EPS	Electronic Power Steering
6.	RAM	Random Access Memory
7.	LA	Lane Assistance
8.	LDW	Lane Departure Warning
9.	LKA	Lane Keeping Assistance

Table of Contents

Purpose

The purpose of the Software Safety Requirements and Architecture Lane Assistance is to define software safety requirements.

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 01-01-01	The LDW safety component shall ensure that the amplitude of the “LDW_Torque_Request” sent to the 'EPS ECU - Final Torque' component is below Max_Torque_Amplitude	C	50 ms	LDW Safety block	LDW torque request shall be set to zero
Technical Safety Requirement 01-01-02	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 request shall be set to zero
Technical Safety Requirement 01-01-03	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 block	LDW torque request shall be set to zero
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for “LDW_Torque_Request” signal shall be ensured	C	50 ms	Data Transmission Integrity Check block	LDW torque request shall be set to zero

Technical Safety Requirement 01-01-05	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 block	LDW torque request shall be set to zero

Refined Architecture Diagram from the Technical Safety Concept

Refined architecture diagram from the technical safety concept is shown in **Figure 1**.

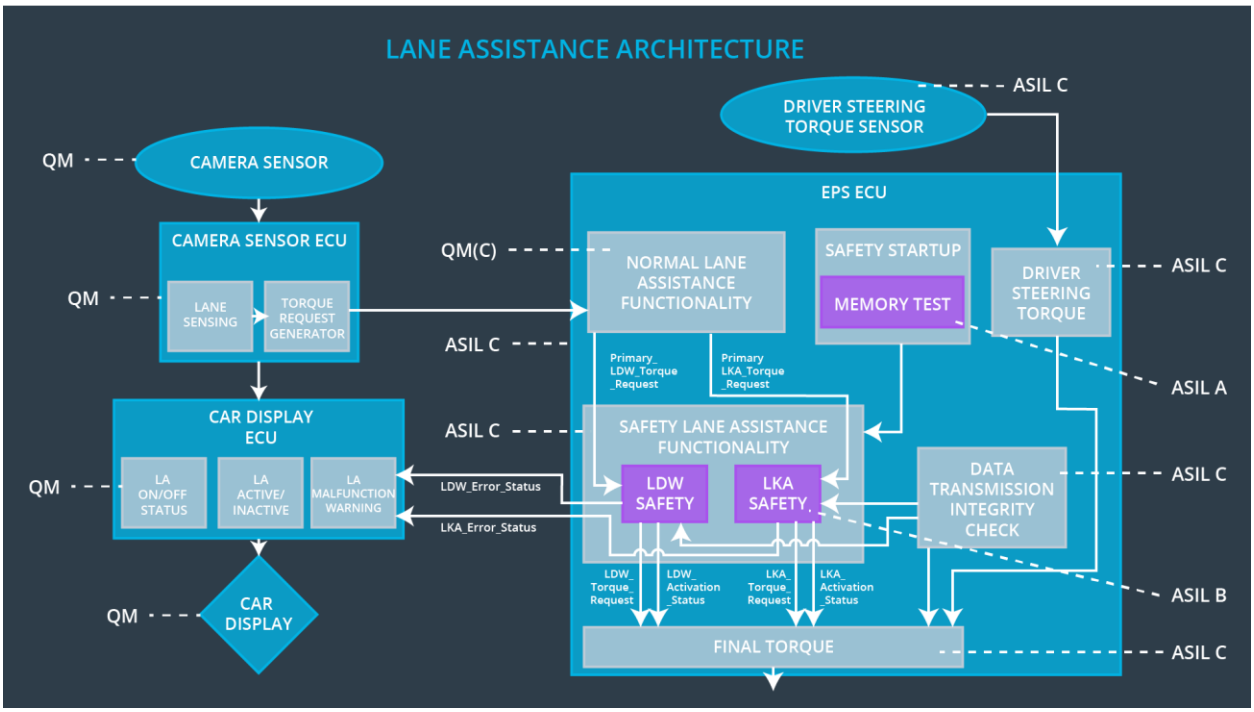

Figure 1

Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

Technical Safety Requirement 01-01-01:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-01	The LDW safety component shall ensure that the amplitude of the “LDW_Torque_Request” sent to the 'EPS ECU - Final Torque' component is below Max_Torque_Amplitude	C	50 ms	LDW Safety block	LDW torque request shall be set to zero

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

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 LAFunctionality’ 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	The “limited_LDW_Torq_Req”shall be transformed into a signal	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req= 0 (Nm)

Requirement 01-03	“LDW_Torq_Req” which is suitable to be transmitted outside of the LDW Safetycomponent (“LDW Safety”) to the “Final EPS Torque” component. Also see SofSafReq 02-01 and SofSafReq 02-02			

Technical Safety Requirement 01-01-02:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-02	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 request shall be set to zero

Software Safety Requirements related to Technical Safety Requirement 01-01-02 are:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01	Each of the software 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
Software Safety Requirement 02-02	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)
Software Safety Requirement 02-03	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
Software Safety Requirement 02-04	In case an error is detected by any of the software elements, it shall set the value of its corresponding torque to 0 so	C	All	LDW_Torq_Req = 0

	that “LDW_Torq_Req” is set to 0			
Software Safety Requirement 02-05	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 Requirement 01-01-03:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-03	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 block	LDW torque request shall be set to zero

Software Safety Requirements related to Technical Safety Requirement 01-01-03 are:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	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

Technical Safety Requirement 01-01-04:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for “LDW_Torque_Request” signal shall be ensured	C	50 ms	Data Transmission Integrity Check block	LDW torque request shall be set to zero

Software Safety Requirements related to Technical Safety Requirement 01-01-04 are:

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	Any data to be transmitted outside of the LDW Safety component (“LDW Safety”) including “LDW_Torque_Req” and “activation_status” (see SofSafReq 02-02) shall be protected by an E2E protection mechanism	C	E2E Calculation	LDW_Torq_Req= 0
Software Safety Requirement 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	E2E Calculation	LDW_Torq_Req= 0

Technical Safety Requirement 01-01-05:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-05	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 block	LDW torque request shall be set to zero

Software Safety Requirements related to Technical Safety Requirement 01-01-05 are:

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 LDW Torque is set to 0	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

Refined Architecture Diagram

Refined architecture diagram is shown in **Figure 2**.

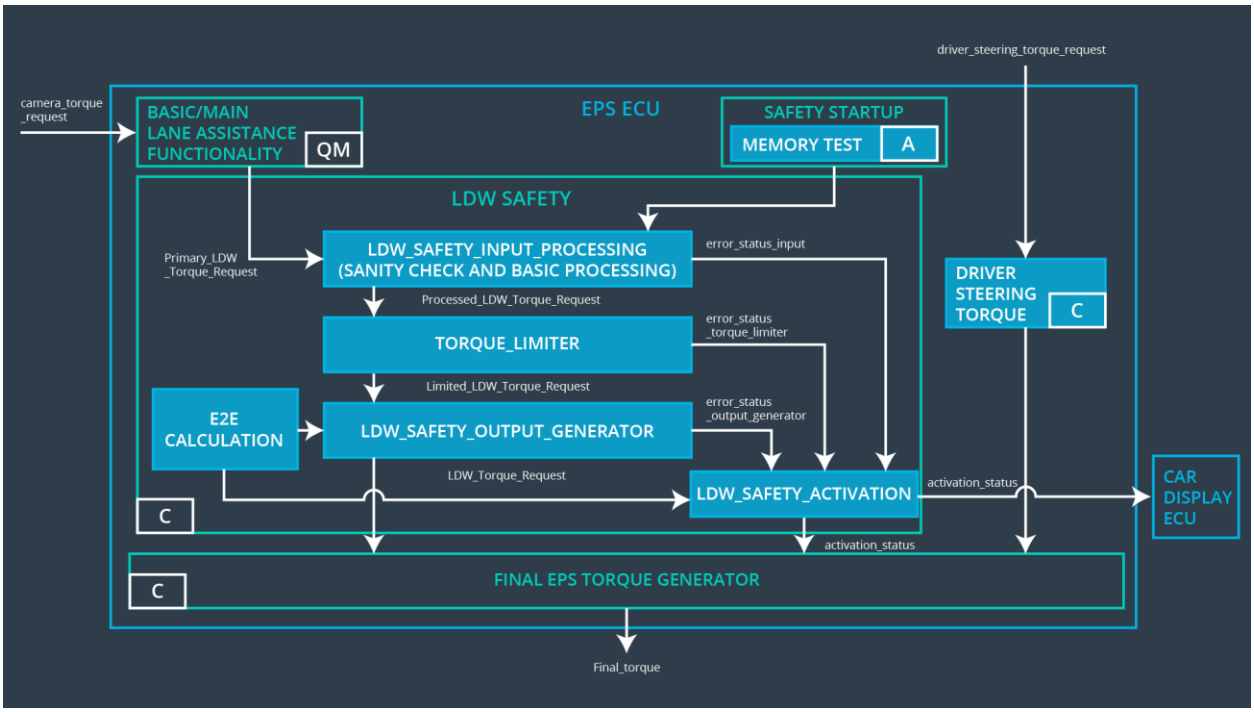

Figure 2