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
11/13/2017	1	JP	First Version
11/27/2017	1.1	JP	Minor changes
12/14/2017	2	JP	Second Version

Table of Contents

Purpose

The purpose of software safety requirements and architecture document is to identify new detailed requirements and allocate these software requirements to component level diagrams for the lane assistance functional safety project that is related to the potential malfunctions of the electrical and electronic system as defined by ISO26262.

Inputs to the Software Requirements and Architecture Document

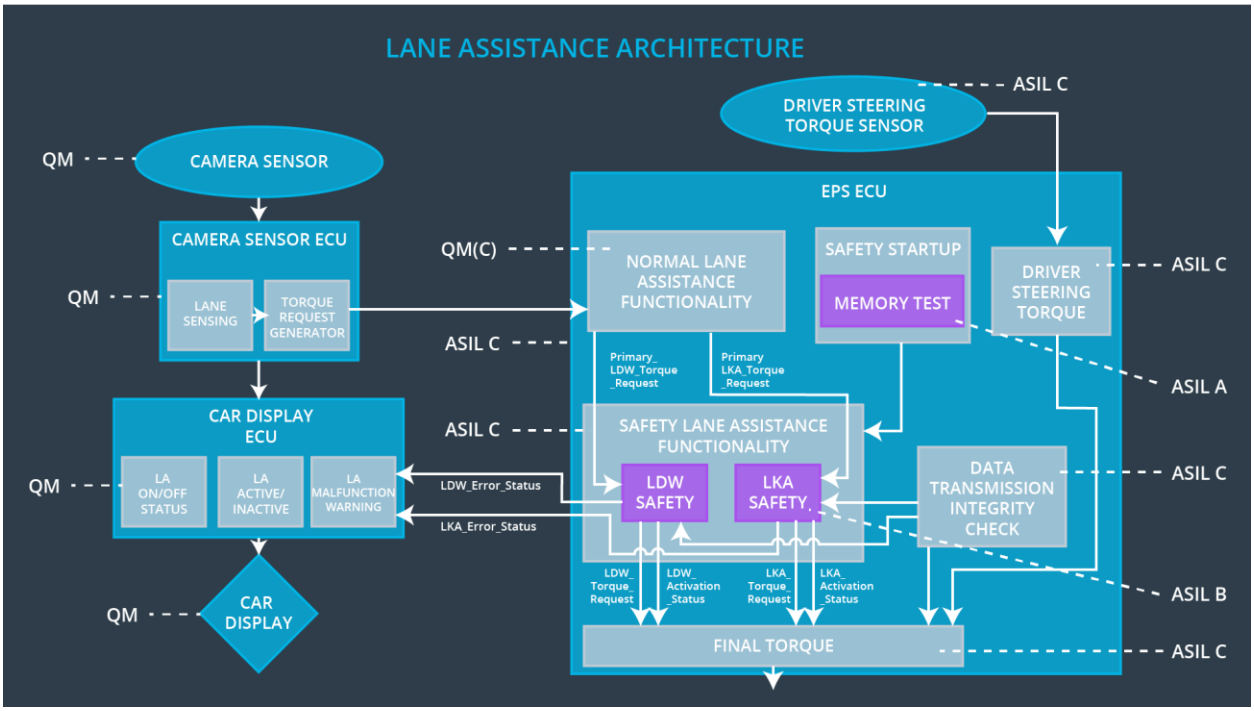
Technical safety requirements

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 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude.	C	50 ms	LDW Safety block	Set LDW torque to zero
Technical Safety Requirement 01-01-02	As soon as the LDW function deactives 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	Set LDW torque to zero
Technical Safety Requirem	As soon as a failure is detected by the LDW function, it shall deactive the LDW feature and	C	50 ms	LDW safety block	Set LDW torque to zero

ent 01-01-03	the ‘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	Set LDW torque 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	Set LDW torque 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 01-01-01	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	Set LDW torque to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-01-01	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	In case the “processed_LDW_Torq_Req” signal has a value greater	C	TORQUE_LIMITER	“limited_LDW_Torq_Req” = 0 (Nm)

Requirement 01-01-01-02	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”.			
Software Safety Requirement 01-01-01-03	The ‘limited_LDW_torque_Request’ shall be transformed into a signal ‘LDW_Torque_Request’ which is suitable to be transmitted outside of the LDW Sefaty component (LDW_SAFETY) to the ‘Final EPS Torque’ component.	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torque_Request = 0 (Nm)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	Data transmission integrity check	Set LDW torque to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-02-01	Any data to be transmittedoutside of the LDW Safetycomponent (“LDW Safety”) including "LDW_Torque_Req"and “activation_status” (seeSofSafReq03-02) shall beprotected by an End2End(E2E) protection mechanism	C	E2ECalc	LDW_Torq_Req= 0 (Nm)
Software Safety Requirement 01-01-02-02	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 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	B	50 ms	LDW Safety block	Set LDW torque to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requiremen 01-01-03-01	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
Software Safety Requirement 01-01-03-02	A software element shall evaluate the error status of all the other software elements and in case any one 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 01-01-03-03	In case of no errors from the software elements, the status of LDW feature shall be set to activated (‘activation_status’ = 1)	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement 01-01-03-04	In case of an error is detected by anu of the software elements, it shall set the value of its corresponding torque to 0 so that ‘LDW_Torque_Request’ is set to 0	C	All	LDW_Torque_Request = 0

Software Safety Requirement 01-01-03-05	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 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	Set LDW torque to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-04-01	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

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	Set LDW torque to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-05-01	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 01-01-05-01	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	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 01-01-05-03	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 01-01-05-04	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