Elektrobit

UDACITY

Software Safety Requirements and Architecture

Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
11/3/2017	1.0	Nicholas Moellers	First Draft

Table of Contents

Purpose

The software requirements document is the last document in the Function Safety Plan. In this document, we will translate technical safety requirements into actual software requirements to be passed on the software engineers for software development. The software safety requirements will specify actual variable names, signal paths, and software protocols and mechanisms.

Inputs to the Software Requirements and Architecture Document

[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.]

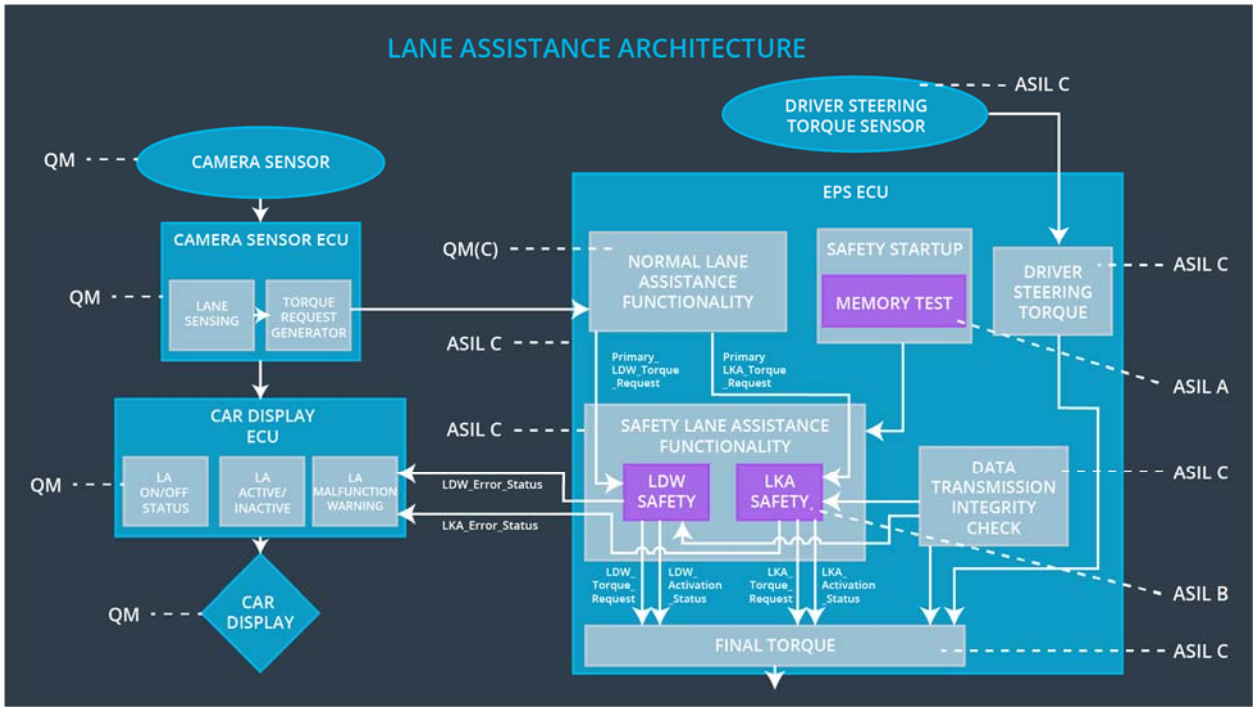
Technical safety requirements

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	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	The "LDW_Torque_Request" Amplitude shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque Request' signal shall be ensured"	C	50 ms	Data Transmission Integrity Check	The "LDW_Torque_Request" Amplitude shall be set to zero
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 be set to zero.	C	50 ms	LDW Safety	The "LDW_Torque_Request" Amplitude 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 ECO to turn on a warning light.	C	50 ms	LDW Safety	The "LDW_Torque_Request" Amplitude shall be set to zero

Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	The “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:

[OPTIONAL:

CHALLENGE ONE
Develop software safety requirements for the Lane Departure Warning (LDW) frequency function and modify the system architecture as needed.

CHALLENGE TWO

Develop software safety requirements for the Lane Keeping Assistance (LKA) function and modify the system architecture as needed.
]

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	50 ms	LDW Safety	The “LDW_Torque_Request” Amplitude shall be set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
SoftwareSafetyRequirement01-01	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
SoftwareSafetyRequirement01-02	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”	C	TORQUE_LIMITER	“limited_LDW_Torq_Req” = 0(Nm=Newton-meter)

	shall take the value of “processed_LDW_Torq_Req”.			
SoftwareSafetyRequirement01-03	The “limited_LDW_Torq_Req”shall be transformed into a signal “LDW_Torq_Req” whichis suitable to be transmittedoutside of the LDW Safetycomponent (“LDW Safety”) to the “Final EPS Torque”component. Also see SofSafReq02-01 andSofSafReq02-02	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

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	50 ms	Data Transmission Integrity Check	The “LDW_Torque_Request” Amplitude shall be set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
SoftwareSafetyRequirement02-01	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)
SoftwareSafetyRequirement02-02	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 be set to zero.	C	50 ms	LDW Safety	The “LDW_Torque_Request” Amplitude shall be set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
SoftwareSafetyRequirement03-01	Each of the SW elements shal loutput 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
SoftwareSafetyRequirement03-02	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 theLDW feature(“activation_status”=0)	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)
SoftwareSafetyRequirement03-03	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
SoftwareSaf	In case an error is detected by	C	All	LDW_Torq_Req = 0

etyRequirement03-04	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			
SoftwareSafetyRequirement03-05	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 ECO to turn on a warning light.	C	50 ms	LDW Safety	The “LDW_Torque_Request” Amplitude shall be set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
SoftwareSafetyRequirement04-01	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 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	The “LDW_Torque_Request” Amplitude shall be set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
SoftwareSafetyRequirement05-01	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
SoftwareSafetyRequirement05-02	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
SoftwareSafetyRequirement05-03	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
SoftwareSafetyRequirement05-04	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	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

	the LDW functionality is deactivated and the LDWTorque is set to 0			

Refined Architecture Diagram