Elektrobit

UDACITY

Software Safety Requirements and Architecture Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
25/12/2018	1.0	Ahmed Desoky	Safety Software requirements and Architecure for Lane Assistance System

Table of Contents

Purpose

This document includes the software requireements from component level. This document is more details oriented that Technical Safety Concept to detect potential safety violations in design or 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.
]

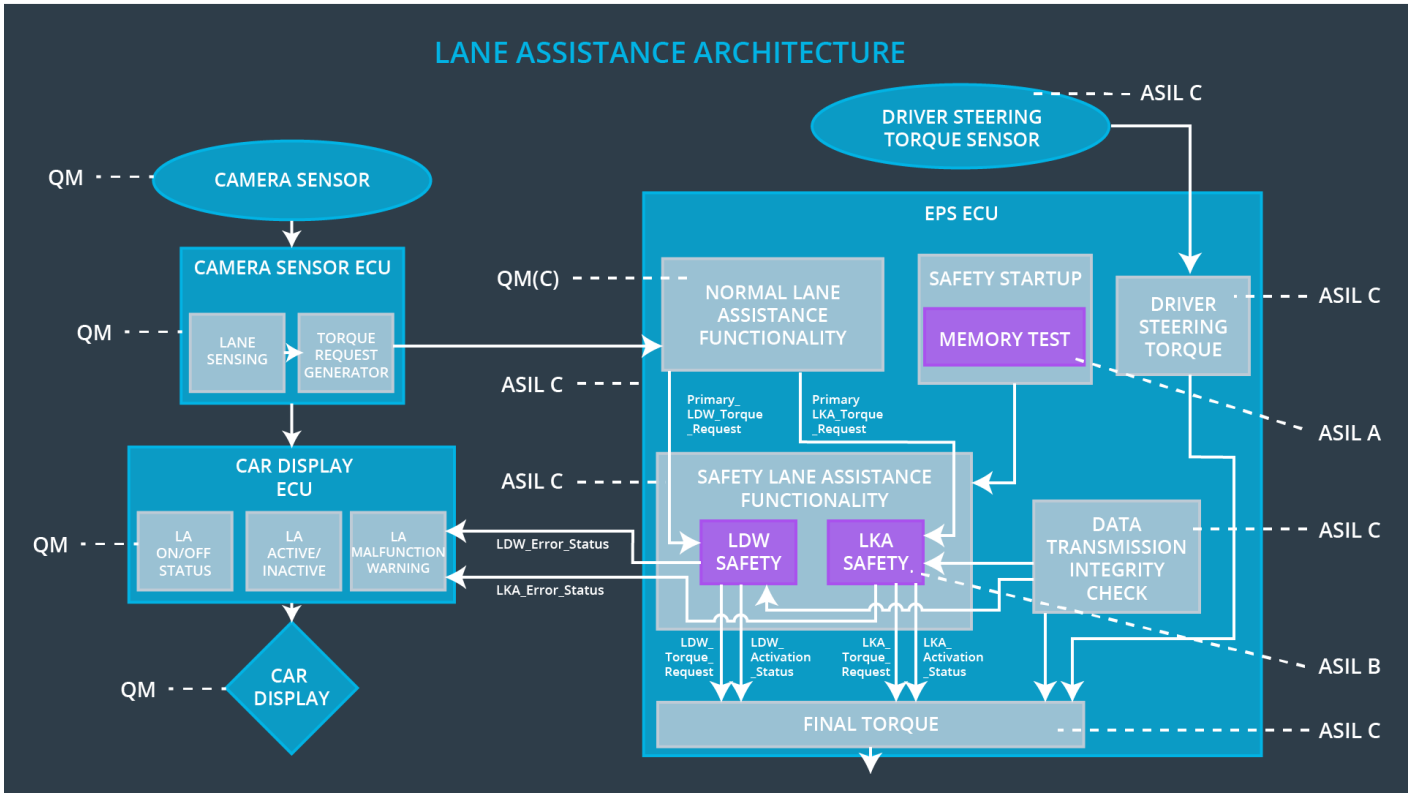
Technical safety requirements

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 01-01-01	The lane departure warning 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	LDW function is deactivated
Technical Safety Requirement 01-01-02	When the LDW is deactivated, the LDW safety SW module shall send a	C	50 ms	LDW Safety	LDW function is deactivated

	signal the car display ECU to activate the warning indicator				
Technical Safety Requirement 01-01-03	When a failure is detected by the LDW functionality, it shall deactivate the LDW feature by setting the “LDW_Torque_Request” by zero	C	50 ms	LDW Safety	LDW function is deactivated
Technical Safety Requirement 01-01-04	The validity and integrity of data sent for “LDW_Torque_Request” shall be ensured	C	50 ms	LDW Safety	LDW function is deactivated
Technical Safety Requirement 01-01-05	Memory test shall be done upon start-up of the EPS ECU to check any memory faults	C	Ignition cycle	Safety Startup	LDW function is deactivated

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 lane departure warning 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	LDW function is deactivated

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-01-01	The input singal “Primary_LDW_Torq_Request” shall be read and pre-processed to determine the torque coming from the “BASIC/MAIN Lane Assistance Functionality” SW component. A signal “Processed_LDW_Torq_Request ” shall be generated after processing	C	LDW_Safety_Input_Processing	N/A
Software Safety Requirement 01-01-01-02	If the value of “Processed_LDW_Torq_Request ” is > Max_Torque_Amplitude, then the value of “LDW_Torque_Request” shall be set to zero. Otherwise, the value of “ LDW_Torque_Request” shall be set to “Processed_LDW_Torq_Request ”	C	Torque_Limiter	LDW_Torque_Request = 0

Software Safety Requirement 01-01-01-03	The singal “LDW_Torque_Request” shall be transferred to the “ Final Torque” component to be sent to the motor in the approperiate format	C	LDW_Torque_Generator	LDW_Torque_Request = 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-02	When the LDW is deactivated, the LDW safety SW module shall send a signal the car display ECU to activate the warning indicator	C	50 ms	LDW Safety	LDW function is deactivated

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-02-01	Any data is sent out of the LDW safety compement shall be protected using End-2-End protection mechanism	C	E2E	LDW_Torque_Request = 0
Software Safety Requirement 01-01-02-02	The E2E mechanism shall apply a cyclic redundcy check (CRC) to check that data is not corrputed	C	E2E	LDW_Torque_Request = 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-03	When a failure is detected by the LDW functionality, it shall deactivate the LDW feature by setting the “LDW_Torque_Request” by zero	C	50 ms	LDW Safety	LDW function is deactivated

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Technical Safety Requirement 01-01-03-01	Any software component or unit inside the LDW Safety SW module detects an error in the processing or calculation shall be able to send an error singal due to invalid input (LDW_Error_Status)	C	All	LDW_Torque_Request = 0
Technical Safety Requirement 01-01-03-02	A software component of the LDW Safety module when detecting an error shall be able to evaluate it to tell the LDW safety SW module to deactive the LDW functionality (LDW_Activation_Status = 0)	C	LDW_Safety	LDW_Actication_Status = 0
Technical Safety Requirement 01-01-03-03	In case of no error evaluated, the LDW_Safety shall set LDW_Activation_Status = 1	C	LDW_Safety	N/A
Technical Safety Requirement 01-01-03-04	Once the LDW functionality is deactivated of an error, it shall be deactivated till the next time of ignition	C	LDW_Safety	LDW_Actication_Status = 0

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 data sent for “LDW_Torque_Request” shall be ensured	C	50 ms	LDW Safety	LDW function is deactivated

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Technical Safety Requirement 01-01-04-01	A cyclic redunduny check (CRC) shall be added with “LDW_Torque_Request” and check when the signal is received by the “Final Torque”	C	Data_trasmission_integrity_Check, LDW_Saferty, Final Torque	LDW_Actication_Status = 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-05	Memory test shall be done upon start-up of the EPS ECU to check any memory faults	C	Ignition cycle	Safety Startup	LDW function is deactivated

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Technical Safety Requirement 01-01-05-01	A CRC check shall be done with every ignition to the code in Flash to make sure that the program is not corrputed	A	Safety Startup	LDW_Actication_Status = 0
Technical Safety Requirement 01-01-05-02	Standard RAM test shall be done for data and address buses and data integrity with every ignition cycle	A	Safety Startup	LDW_Actication_Status = 0
Technical Safety Requirement 01-01-05-03	Test result shall be indicated to the LDW_Safety component via “test_result” signal	A	Safety Startup , LDW_Safety	N/A
Technical Safety Requirement 01-01-05-03	In case test result has erros, the LDW_torque_Req shall be set to 0	A	Safety Startup , LDW_Safety	LDW_Actication_Status = 0
Technical Safety Requirement 01-01-05-04	In case test result has erros, the LDW_Error_Status shall be set to 1 to indicate to the user on the dashboard that there is a problem		Safety Startup , LDW_Safety	LDW_Actication_Status = 0

Refined Architecture Diagram