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
03/03/2019	1.0	Rangarajan Ramanujam	Initial Draft

Table of Contents

Purpose

This document identifies new requirements for the software at component level to identify potential problems on software design and architecture that could lead to a violation of safety goals. These requirements are oriented to provide more detail than the technical safety concept 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 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 Torque Request Amplitude shall be set to zero
Technical Safety Requirement 01-01-02	When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal	C	50 mS	LDW Safety	LDW Torque Request Amplitude shall be set to zero
Technical Safety Requirement 01-01-03	When 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	LDW Torque Request Amplitude 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	LDW Safety	LDW Torque Request Amplitude shall be set to zero
Technical Safety Requirement	Memory test shall be conducted at startup of the	A	Ignition Cycle	Data Transmission Integrity	LDW Torque Request Amplitude

01-01-05	EPS ECU to check for any faults in memory			Check	shall be set to zero

Refined Architecture Diagram from the Technical Safety Concept

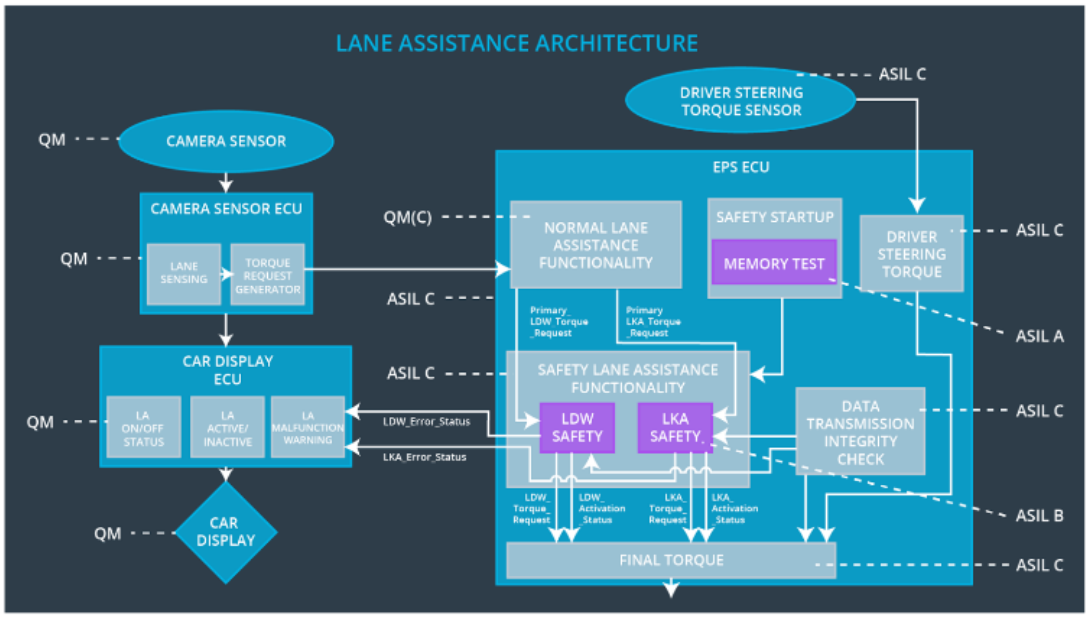

Fig 1: Refined Architecture Diagram from Technical Safety Concept

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	C	50 mS	LDW Safety	Lane Departure Warning torque to zero

	Max_Torque_Amplitude				

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 Requirement 01-01-01-02	In case the ‘processed_LDW_Torq_Req’ signal has a value greater than ‘Max_torque_Amplitude_LDW’ (maximum allowed safe torque), the torque signal ‘limited_LDW_Torq_Req’ shall take the value of ‘processed_LDW_Torq_Req’	C	TORQUE_LIMITER	limited_LDW_Torq_Req = 0 Nm
Software Safety Requirement 01-01-01-03	The ‘limited_LDW_Torq_Req’ shall be transformed into a signal ‘LDW_Torq_Req’ which is suitable to be transmitted outside the LDW Safety Component(‘LDW Safety’) to the ‘Final EPS Torque’ component	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 01-01-02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 mS	LDW Safety	Lane Departure Warning torque is set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-02-01	When the Lane departure warning function is deactivated(‘activation_status =0), the activation_status shall be sent to the Car Display ECU	C	LDW_SAFETY_ACTIVATION, Car Display ECU	N/A

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	Lane Departure Warning torque to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-03-01	Each software element 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 other software elements and in case any one of them indicates an error, it shall deactivate the Lane departure Warning feature (‘activation_status = 0’)	C	LDW_SAFETY_ACTIVATION	Lane Departure Warning function deactivated(‘activation_status = 0’)
Software Safety Requirement 01-01-03-03	In case of a no error from the software elements, the status of the Lane departure warning feature shall be set to activated (‘activation_status = 1’)	C	LDW_SAFETY_ACTIVATION	N/A
Software	In case an error is detected by	C	All	LDW_Torq_Req = 0

Safety Requirement 01-01-03-04	any of the software elements, it shall set the value of its coresponding torque to zero so that ‘LDW_Torq_Req’ is set to zero			
Software Safety Requirement 01-01-03-05	Once the Lane Departure Warning functionality has been deactivated, it shall stay deactivated until the time the ignition is switched from off to on again.	C	LDW_SAFETY_ACTIVATION	Lane Departure Warning function deactivated(‘activation_status = 0’)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-04	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 signal	C	50 mS	LDW Safety	Lane Departure Warning torque to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-04-01	Any data to be transmitted outside the LDW Safety Component including 'LDW_Torque_Req' and 'activation_status' shall be protected by an End-2-End protection mechanism	C	E2C Calc	LDW_Torq_Req = 0 Nm
Software Safety Requirement 01-01-04-02	The E2E protection protocol shall contain and attach the control data(alive counter SQC and CRC) to the data to be transmitted	C	E2C Calc	LDW_Torq_Req = 0 Nm

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 startup of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Data Transmission Integrity Check	Lane Departure Warning torque is set 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 content corruption	A	MEMORYTEST	Activation_Status = 0
Software Safety Requirement 01-01-05-02	Standard RAM test to check the data bus, the address bus and device integrity shall be done every time the ignition is switched from off to on (eg: walking 1s test, RAM pattern test, Refer to RAM and processor vendor recommendations)	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 the error_status_input(=1) so that the Lane Departure Warning functionality is deactivated and the LDW_Torq_Req is set to zero	A	LDW_SAFETY_INPUT_PROCESSING	Activation_Status = 0

Refined Architecture Diagram

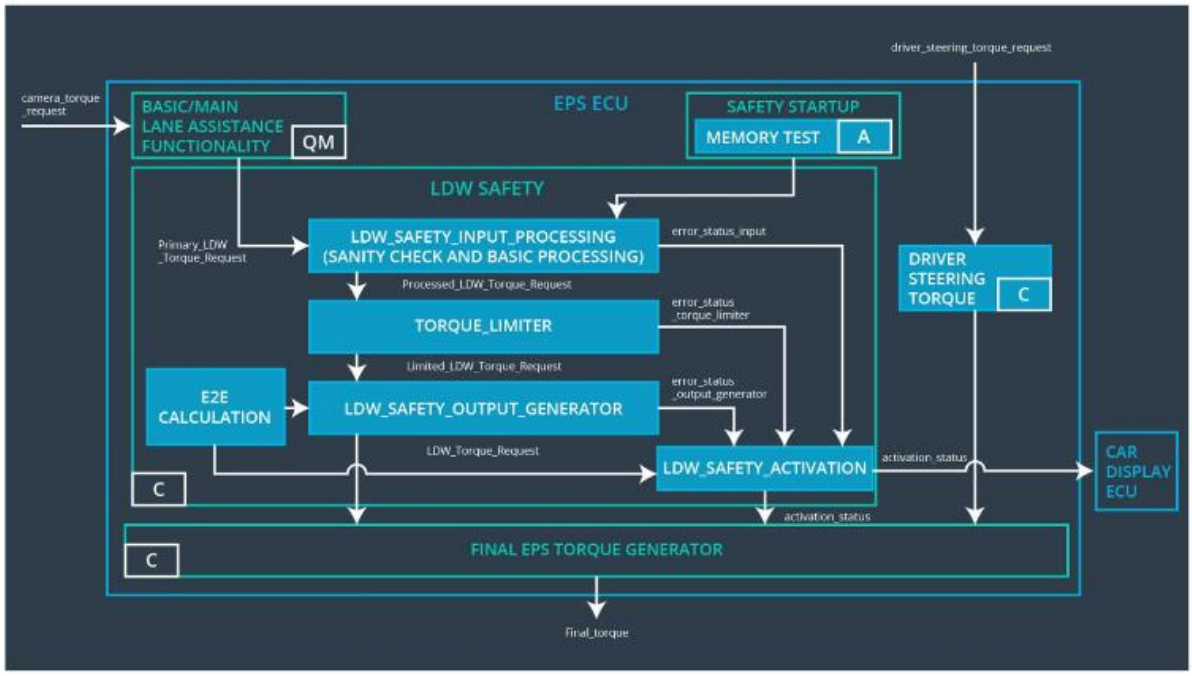

Fig 2: Refined Architecture Diagram With ASIL Levels defined