Elektrobit

UDACITY

Software Safety Requirements and Architecture

Lane Assistance

Document Version: 2.0

Document history

Date	Version	Editor	Description
Aug 21, 2017	1.0	Jian Liang Linn	Initial Draft
Aug 22, 2017	2.0	Jian Liang Linn	1) Corrected technical requirements 01-01-02 and 01-01-03 2) Filled the ASIL level as 'A' in software safety requirements 01-01-05-03 and 01-01-05-04

Table of Contents

Purpose

This document identifies new detailed software requirements and allocate these requirements to component levels for the lane assistance functional safety project as defined by ISO 26262 standard.

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 the torque amplitude of the LDW_TORQUE_REQUEST sent to the EPS Torque component is below MAX_TORQUE_AMPLITUDE	C	50 ms	LDW Safety	Set lane departure warning torque to zero
Technical Safety Requirement 01-01-02	The LDW Safety Software shall send a signal to the Car Display ECU to turn on a warning light when the LDW function detect a failure	C	50 ms	LDW Safety	Set lane departure warning torque to zero
Technical Safety Requirement 01-01-03	The LDW feature is deactivated when the LDW function detects a failure and the LDW_TORQUE_REQUEST shall be set to zero	C	50 ms	LDW Safety	Set lane departure warning torque to zero

Technical Safety Requirement 01-01-04	The LDW_TORQUE_REQUEST data signal validity and integrity shall be ensured	C	50 ms	LDW Safety	Set lane departure warning toque to zero
Technical Safety Requirement 01-01-05	Any memory faults test shall be conducted at the startup of the EPS ECU	A	Ignition cycle	Data transmission integrity	Set lane departure warning to zero
Technical Safety Requirement 01-02-01	The torque frequency request that sent to EPS Torque component shall be ensured below the MAX_TORQUE_FREQUENCY	C	50 ms	LDW Safety	Set lane departure warning torque to zero

Refined Architecture Diagram from the Technical Safety Concept

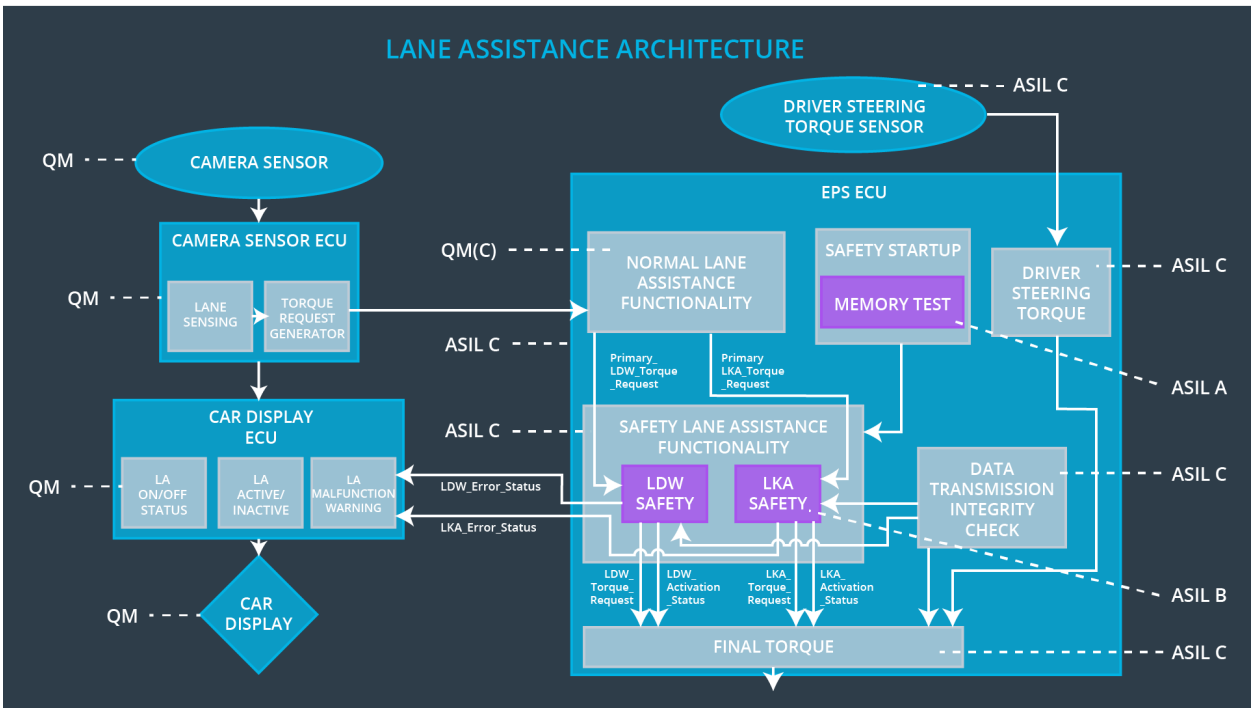

figure 1: Refined System Architecture

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 the torque amplitude of the LDW_TORQUE_REQUEST sent to the EPS Torque component is below MAX_TORQUE_AMPLITUDE	C	50 ms	LDW Safety	Set lane departure warning torque to zero

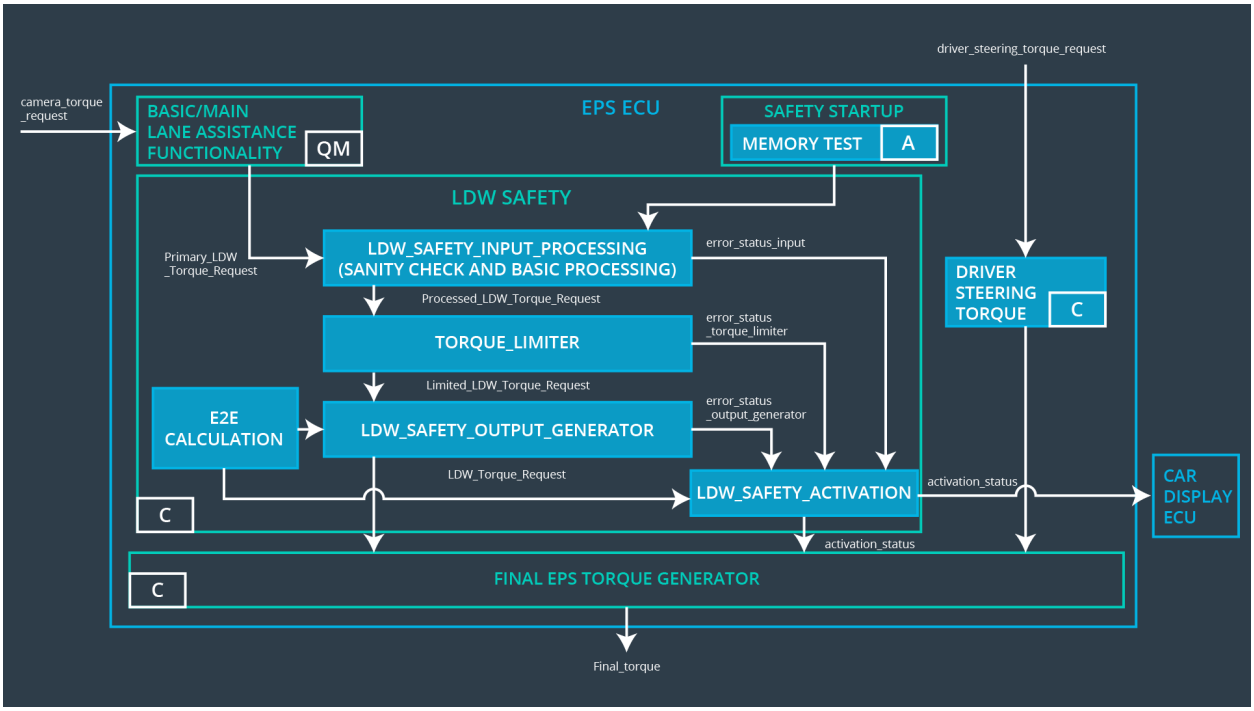

figure 2: Software Components Daigram

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-01-01	The signal Primary_LDW_Torque_Request shall be read and pre-processed the request comes from Basic/Main LANE ASSISTANCE FUNCTIONALITY component and the signal Processed_LDW_Torque_Request shall be generated after the processing	C	LDW_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 01-001-01-02	The Limited_LDW_Torque_Request shall be set to zero when Processed_LDW_Torque_Request has value greater than MAX_TORQUE_AMPLITUDE_LDW otherwise, Limited_LDW_Torque_Request shall use the value of Processed_LDW_Torque_Request	C	TORQUE_LIMITER	Limited_LDW_TORQUE_Request = 0
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 Safety Component to the Final EPS Torque component	C	LDW_SAFETY_OUTPUT_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	The LDW Safety Software shall send a signal to the Car Display ECU to turn on a warning light when the LDW function detect a failure	C	50 ms	LDW Safety	Set lane departure warning torque to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-02-01	The activation_staus shall be sent to the Car Display ECU when the LDW function is deactivated	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	The LDW feature is deactivated when the LDW function detects a failure and the LDW_TORQUE_REQUEST shall be set to zero	C	50 ms	LDW Safety	Set lane departure warning torque to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-03-01	Every SW elements shall output a signal when any errors (preceding) are detected by the element. 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	When any error is detected by one of any software elements, the software element 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	The LDW feature shall be activated (activation_status = 1) if there is no error detected by any software elements.	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement 01-01-03-04	When any error is detected by one of any software elements, the software element shall set the corresponding torque to be zero (LDW_TORQUE_REQUEST = 0)	C	All	LDW_TORQUE_REQUEST = 0

Software Safety Requirement 01-01-03-05	Once the LDW feature has been deactivated, it shall remain deactivated until restarting of ignition	C	LDW_SAFETY_ACTIVATION	activation_status = 0 (LDW feature deactivated)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-04	The LDW_TORQUE_REQUEST data signal validity and integrity shall be ensured	C	50 ms	LDW Safety	Set lane departure warning toque 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 of the LDW Safety component including LDW_TORQUE_REQUEST and activation_status shall be protected by E2E protection module	C	E2E CALCULATION	LDW_TORQUE_REQUEST = 0
Software Safety Requirement 01-01-04-02	E2E protection protocol shall contain the data integrity check sum (CRC) and sequence counter (SQC) in the transmitted data	C	E2E CALCULATION	LDW_TORQUE_REQUEST = 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-05	Any memory faults test shall be conducted at the startup of the EPS ECU	A	Ignition cycle	Data transmission integrity	Set lane departure warning to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-05-01	Object code in the flash memory shall be checked every single ignition on.	A	MEMORY TEST	activation_status = 0
Software Safety Requirement 01-01-05-02	The RAM test of data and address buses and all devices integrity check shall be done every time ignition is on	A	MEMORY TEST	activation_status = 0
Software Safety Requirement 01-01-05-03	The test status shall be set to the LDW SAFETY component from SAFETY STARTUP component	A	MEMORY TEST	activation_status = 0
Software Safety Requirement 01-01-05-04	The error_status_input shall be set to one in case of any fault is indicated via test status signal to deactivate LDW functionality and to set LDW Torque to be zero	A	MEMORY TEST	activation_status = 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State

Technical Safety Requirement 01-02-01	The torque frequency request that sent to EPS Torque component shall be ensured below the MAX_TORQUE_FREQUENCY	C	50 ms	LDW Safety	Set lane departure warning torque to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-02-01-01	The signal Primary_LDW_Torque_Request shall be read and pre-processed the request comes from Basic/Main LANE ASSISTANCE FUNCTIONALITY component and the signal Processed_LDW_Torque_Request shall be generated after the processing	C	LDW_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 01-02-01-02	The Limited_LDW_Torque_Request shall be set to zero when Processed_LDW_Torque_Request has value greater than MAX_TORQUE_AMPLITUDE_LDW otherwise, Limited_LDW_Torque_Request shall use the value of Processed_LDW_Torque_Request	C	TORQUE_LIMITER	Limited_LDW_TORQUE_Request = 0
Software Safety Requirement 01-02-01-03	The Limited_LDW_Torque_Request shall be transformed into a signal LDW_Torque_Request which is suitable to be transmitted outside of the LDW Safety Component to the Final EPS Torque component	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torque_Request = 0

Refined Architecture Diagram

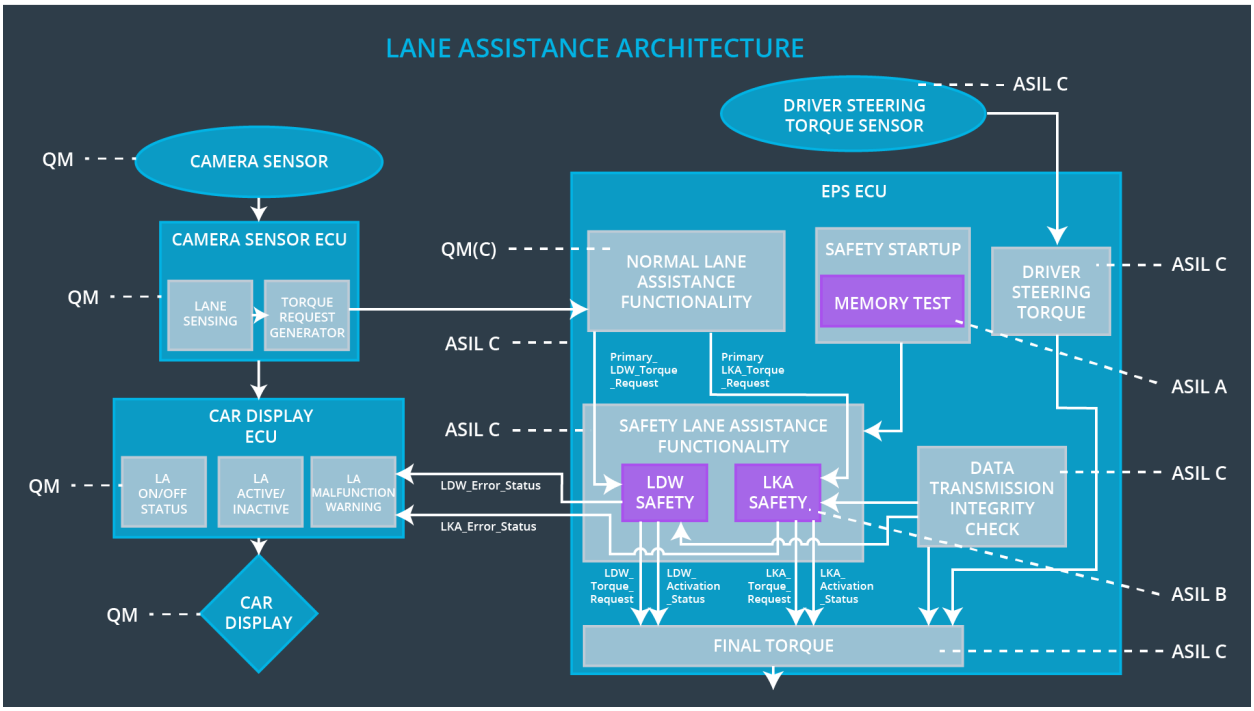

figure 3: Refined Overall Architecture

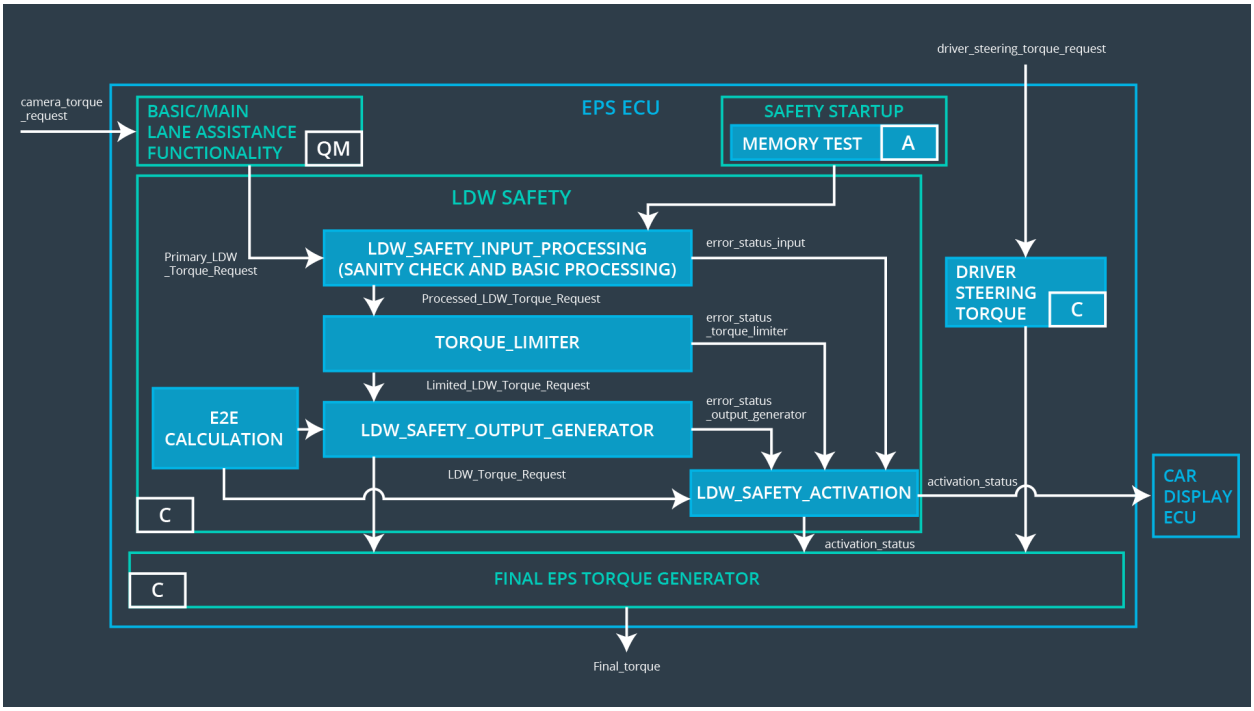

figure 4: Overall Software Component Diagram