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
10/15/2018	1.0	John O’Shea	Initial Draft

Table of Contents

Purpose

The purpose of the document is to document detailed software safety requirements using the technical safety requirments.

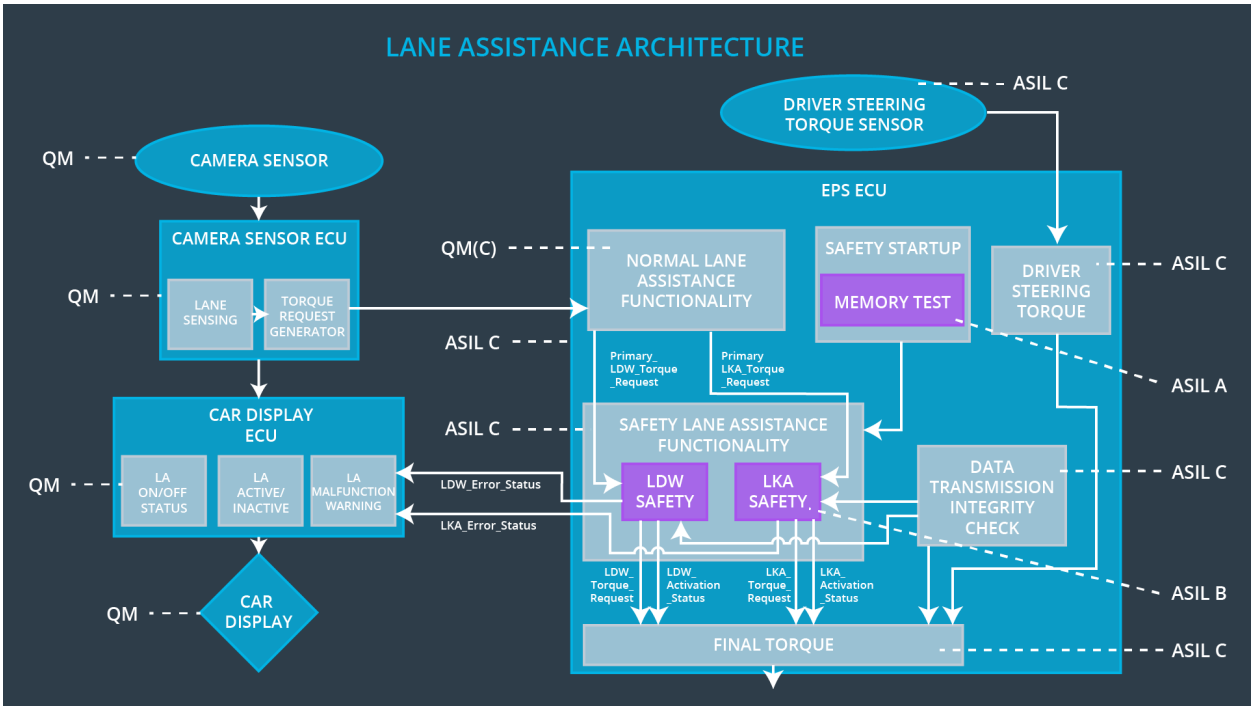
Inputs to the Software Requirements and Architecture Document

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	The LDW component shall ensure that the LDW_Torque_Request for lane departure warning is below Max_Torque_Amplitude.	C	50 ms	LDW Safety	The LDW torque amplitude is set to 0.
Technical Safety Requirement 02	When the LDW feature is deactivated, the LDW software component shall block any requests to activate a warning light to the car display ECU	C	50 ms	LDW Safety	The LDW torque amplitude is set to 0.
Technical Safety Requirement 03	Once a failure is detected the LDW feature is deactivated and a torque request shall not be sent.	C	50 ms	LDW Safety	The LDW torque amplitude is set to 0.
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request shall be checked	C	50 ms	Data Transmission Integrity check	The LDW torque amplitude is set to 0.
Technical Safety Requirement 05	A memory test shall be conducted during the start up of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Memory Test	The LDW torque amplitude is set to 0.

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	The LDW component shall ensure that the LDW_Torque_Request for lane departure warning is below Max_Torque_Amplitude.	C	50 ms	LDW Safety	The LDW torque amplitude is set to 0.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01	The input signal ‘Primary_LDW_Torque_Request’ shall be read and pre-processed to determine the torque request coming from the ‘Basic/Main LANE Assistance Funtionality’ SW component. The signal ‘Processed_LDW_Torque_Request’ shall be generated at the end of processing.	C	LDW_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 01-02	If ‘Processed_LDW_Torque_Request’ has a value greater than ‘Max_Torque_Amplitude_LDW’ , the torque signal ‘Limited_LDW_Torque_Request’ shall be set to zero, else ‘Limited_LDW_Torque_Request’ shall take the value of the ‘Processed_LDW_Torque_Request’	C	TORQUE_LIMITER	limited_LDW_Torque_Request = 0
Software Safety Requirement 01-03	The ‘Limited_LDW_Torque_Request’ shall be transformed into a signal ‘LDW_Torque_Request’ 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 torque amplitude set to 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02	When the LDW feature is deactivated, the LDW software component shall block any requests to activate a warning light to the car display ECU	C	50 ms	LDW Safety Data Transmission Integrity check	The LDW torque amplitude is set to 0.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01	When the LDW function is deactivated (activation_status=0), and further requests shall first check activation_status before sending requests	C	All SW Elements	The LDW torque amplitude is set to 0.
Software Safety Requirement 02-02	When the LDW function is deactivated (activation_status=0), the activation_status shall be sent to the Car Display ECU to enable the Car Display warning light	C	Car Display ECU, Car Display	activation_status=0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 03	Once a failure is detected the LDW feature is deactivated and a torque request shall not be sent.	C	50 ms	LDW Safety	The LDW torque amplitude is set to 0.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	Each SW element detecting an error shall assert its error signal to indicate an error was detected.	C	All SW elements with error outputs	N/A
Software Safety Requirement 03-02	Each SW element shall check for errors asserted by other elements and if an error is detected it shall deactivate the LDW feature. (activation_status=0)	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement 03-03	Each SW element shall check for errors asserted by other elements and if an error is not detected it shall assert keep LDW feature activated. (activation_status=1)	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement 03-04	If an error is detected by any SW element the LDW_Torque_Request shall be set to 0	C	All SW elements with error outputs	LDW_Torque_Request = 0
Software Safety Requirement 03-05	If the LDW is deactivated, it shall stay deactivated until the vehicle is shut off and restarted	C	LDW_SAFETY_ACTIVATION	activation_status=0

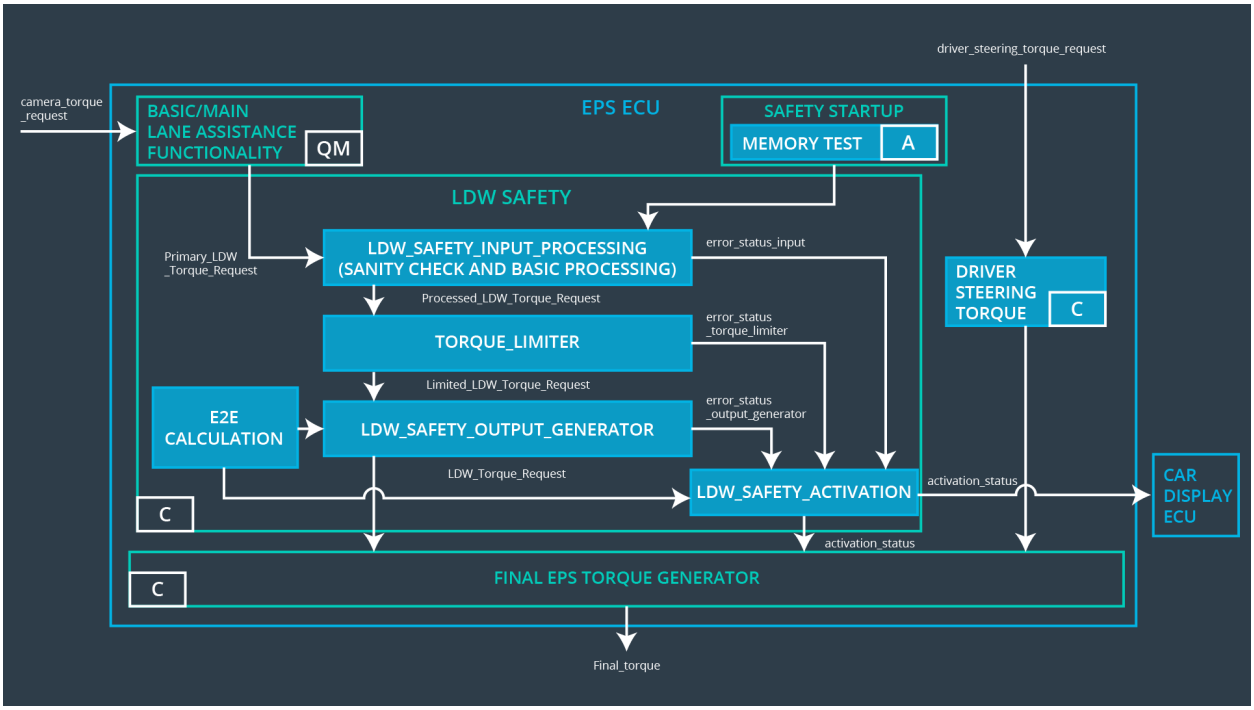
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request shall be checked	C	50 ms	Data Transmission Integrity check	The LDW torque amplitude is set to 0.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	All data transmitted outside of “LDW Safety” shall be protected with End2End(E2E) protection. The E2E shall be activated for header/payload portions of each data packet	C	E2E Calculation	LDW_Torque_Request is set to 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	A memory test shall be conducted during the start up of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Memory Test	The LDW torque amplitude is set to 0.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 05-01	A BIST memory test shall be run to test data and address busses using various patterns to validate the integtrity of the memory system	A	MEMORY_TEST	activation_status=0
Software Safety Requirement 05-02	A CRC shall be computed for SW requests packets between ECUs	A	MEMORY_TEST	activation_status=0
Software Safety Requirement 05-03	Any error detected by the MEMORY_TEST shall be propogated to the LDW_Safety_component	A	MEMORY_TEST	activation_status=0
Software Safety Requirement 05-04	Any error detected by the MEMORY_TEST shall cause the LDW_Safety_Activation component to set activation_status=0	A	LDW_SAFETY_ACTIVATION	activation_status=0

Refined Architecture Diagram



[