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
10-28-18	1.0	Madhukar	First Draft

Table of Contents

Purpose

This document identify the new requirements for the software components at a component level to identify potential problems on software design and architecture that could lead to a violation of safety goals. These requirements are more detail oriented than the technical safety concept requirements.

Inputs to the Software Requirements and Architecture Document

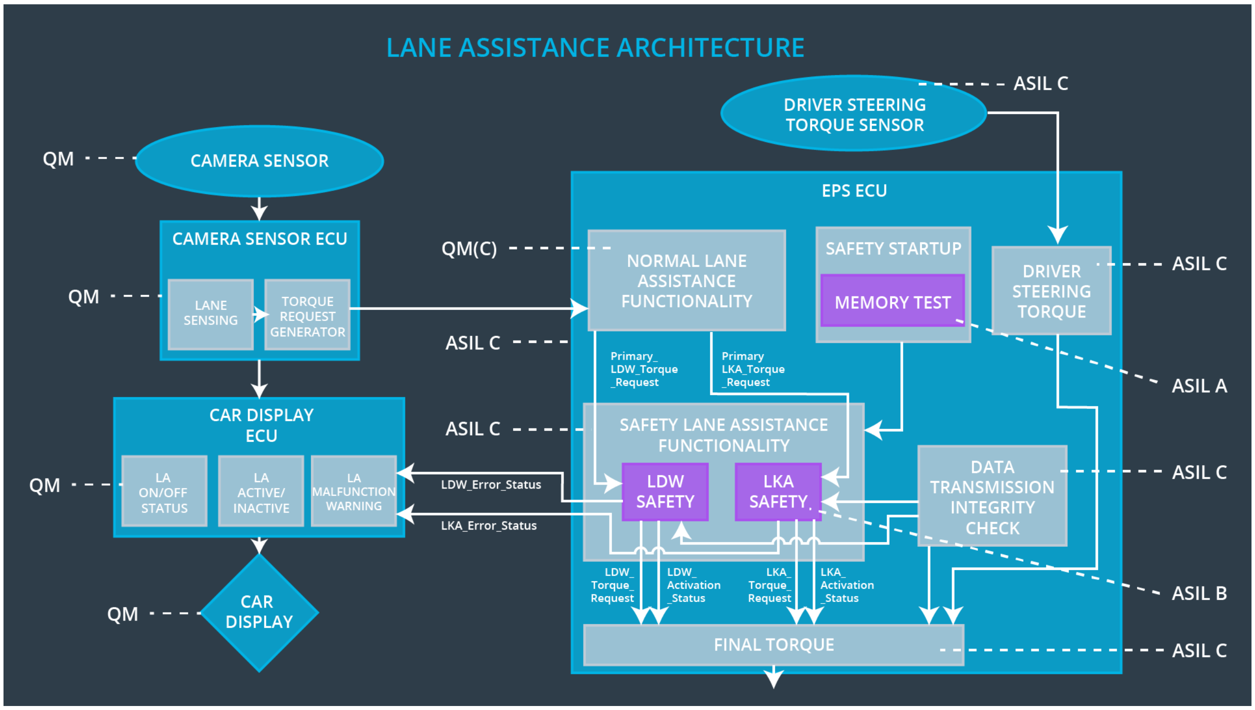
Technical safety requirements

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	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 Amplitude = 0
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	LDW Safety	LDW Torque Amplitude = 0
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	LDW Torque Amplitude = 0
Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to	C	50 ms	LDW Safety	LDW Torque Amplitude = 0

	the car display ECU to turn on a warning light.				
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Data Transmission Integrity Check	LDW Torque Amplitude = 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 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 Output = 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 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	NA
Software Safety Requirement 01-02	In case the “Processed_LDW_Torq_Req” signal has a value greater than “Max_Torque_Amplitude_LDW” the torque signal “Limited_LDW_Torq_Req” shall be set to 0, else “Limited_LDW_Torq_Req” shall take the value of	C	Torque_Limiter	Limited_LDW_Torque_Req = 0

	“processed_LDW_Torq_Req”			
Software Safety Requirement 01-03	The “limited_LDW_Torq_Req” shall be transformed into a signal “LDW_Torq_Req” which is suitable to be transmitted outside of the LDW Safety component (“LDW Safety”) to the “Final EPS Torque”component.	C	LDW_Safety_Output_Generator	LDW Torque Req = 0

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	LDW Safety	LDW torque output = 0

ID	**Software Safety Requirement**	**ASIL**	**Allocation Software Elements**	**Safe State**
Software Safety Requirement 02-01	Any data to be transmitted outside of the LDW Safety component (“LDW Safety”) including "LDW_Torque_Req" and “activation_status” shall be protected by an E2E protection mechanism	C	E2ECalc	LDW Torque Req = 0
Software Safety Requirement 02-02	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

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	LDW Torque Output = 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	Each of the SW elements shall output a signal to indicate any error which is detected by the element. Error signal = error_status_input, error_status_torque_limiter, error_status_output_gen	C	All	NA
Software Safety Requirement 03-02	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 the LDW feature		LDW_Safety_Activation	Activation_status = 0
Software Safety Requirement 03-03	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	LDW_Torq_Req = 0
Software Safety Requirement 03-04	In case an error is detected by 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	C	All	NA
Software Safety Requirement 03-05	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

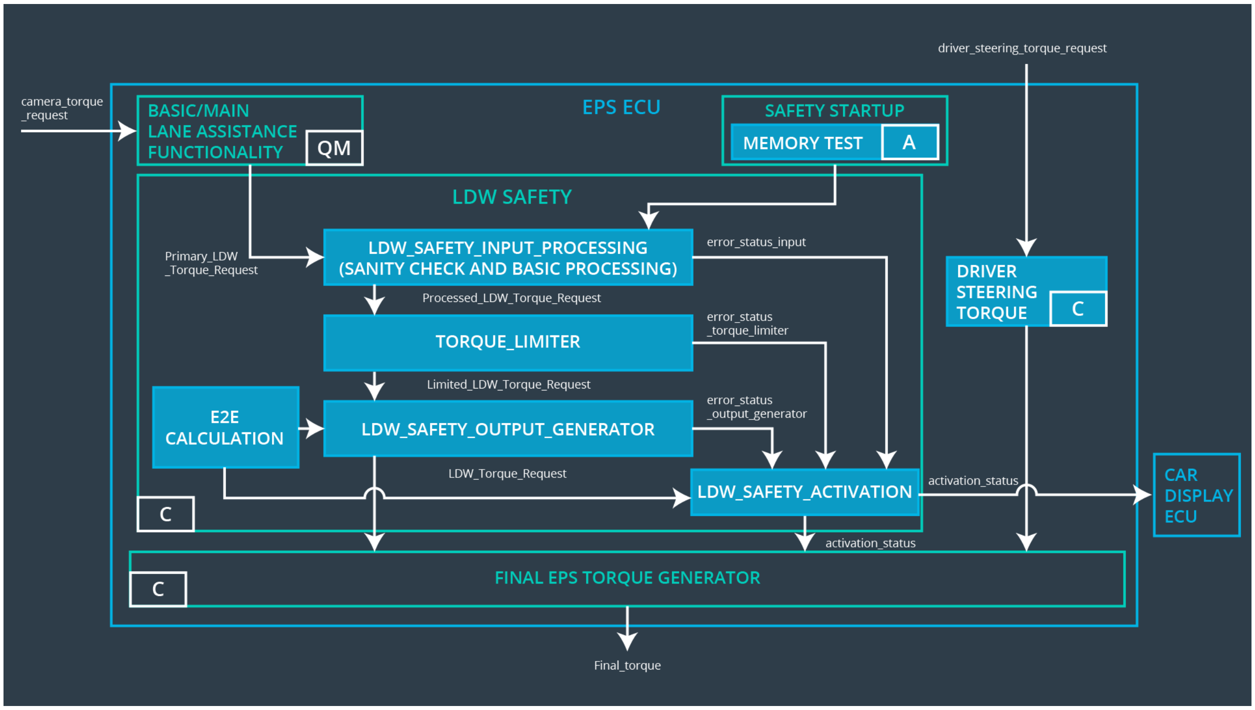
ID	Technical Safety Requirement	A S I L	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light	C	50 ms	LDW Safety	LDW Torque Output = 0

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	When the LDW function is deactivated (activation_status set to 0), the activation_status shall be sent to the car display ECU.	C	LDW_Safety_ Activation, Car Display ECU	NA

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Memory Test	LDW Torque Output = 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 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 corruption of content	A	Memory Test	Activation_Status = 0
Software Safety Requirement 05-02	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	A	Memory Test	Activation_Status = 0
Software Safety Requirement 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	Memory Test	Activation_Status = 0
Software Safety Requirement 05-04	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 the LDW functionality is deactivated and the LDW_Torque is set to 0		LDW_Safety_Input_Processing	Activation_Status = 0

Refined Architecture Diagram


driver_steering_torque_request
camera_torque
_request
BASIC/MAIN
LANE ASSISTANCE
FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW
_Torque_Request
LDW_SAFETY_INPUT_PROCESSING
(SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER
STEERING
TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status
_torque_limiter
Limited_LDW_Torque_Request
E2E
CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status
_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR
DISPLAY
ECU
C
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque