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
03/03/2019	V1.0	Madhu Hegde	First Version

Table of Contents

Purpose

The purpose of this document is to specify software requirements at a component level. The requirements are specified to identify potential problems in the software design and architecture that could lead to a violation of safety goals. The software requirements are more detail oriented than the technical safety concept requirements.

Inputs to the Software Requirements and Architecture Document

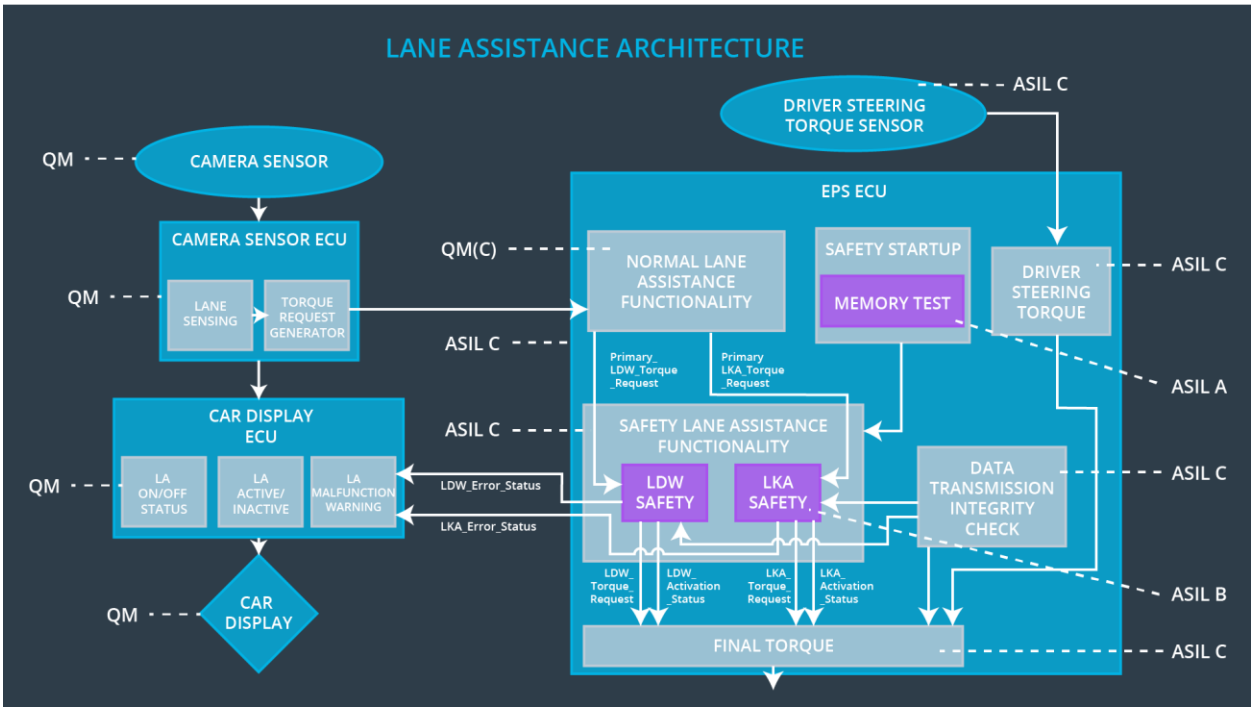
Technical safety requirements

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	Lane Departure
Technical Safety Requirement 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	Lane Departure Warning torque to zero.
Technical Safety Requirement 03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.

	zero.				
Technical Safety Requirement 04	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 to zero.
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

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	Lane Departure Warning torque to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01	The input signal ‘Primary_LDW_Torq_Req’ from the ‘Basic/Main LAFunctionality’ SW Component shall be processed to generate Signal ‘processed_LDW_Torq_Req’.	C	LDW_SAGETY_INPUT_PROCESSING	N/A
Software Safety Requirement 01-02	If the ‘processed_LDW_Torq_Req’ signal is greater than ‘Max_Torque_Amplitude_LDW’, ‘limited_LDW_Torq_Req’ value shall be set to zero, else ‘limited_LDW_Torq_Req’ shall	C	TORQUE_LIMITER	‘limited_LDW_Torq_Req’ = 0 (Nm=Newton-meter)

	take the value of ‘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 conditioned 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 02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured				

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01	Any data to be transmitted outside the LDQ Safety component (‘LDW Safety’) including ‘LDW_Torque_Req’ and ‘activation_status’ shall be protected by an End-2-End protection mechanism.	C	End2End Calc	LDW_Torq_Req = 0 (Nm)
Software Safety Requirement 02-02	The E2E protection protocol shall contain and attach the control data: alive counter (SQC) and CRC/checksum to the data to be transmitted	C	End2End Calc	LDW_Torq_Req = 0 (Nm)

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	Lane Departure Warning torque to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	Each Software component shall output a signal to indicate any error 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 03-02	A software element shall evaluate error status of all other software elements. If 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 03-03	The status of the Lane Departure Warning feature shall be set to activated (‘activation_status’=1) if there is no error from other software elements,	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety	If an error is detected by any of the software elements,	C	All	LDW_Torq_Req = 0

Requirement 03-04	corresponding torque value is set to zero by setting 'LDW_Torq_Req' to zero			
Software Safety Requirement 03-05	Once the Lane Departure Warning functionality has been deactivated, it shall stay deactivating until 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 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	Lane Departure Warning torque to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	When the Lane Departure Warning function is deactivated ('activation_status' set to zero), 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 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	Lane Departure Warning torque to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 05-01	A CRC checksum verification of 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 05-02	Standard RAM test to check the data bus, address bus and device integrity shall be done every time the ignition is switched from off to on (e. G. walking 1s test, RAM pattern test, Refer to RAM and processor vendor recommendations)	A	MEMORYTEST	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	MEMORYTEST	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 the error_status_input(=1) so that the Lane Departure Warning functionality is deactivated and the LDW_Torque_Req is set to zero.	A	LDW_SFETY_INPUT_PROCESSING	Activation_status = 0

Refined Architecture Diagram