Software Safety Requirements and Architecture

Lane Assistance

Document Version: 4.0
Released on 2017-10-31

Document history

Date	Version	Editor	Description
10-23-2017	1.0	Brian McHugh	Set up template
10-26-2017	2.0	Brian McHugh	First draft
10-29-2017	2.0	Brian McHugh	Complete up to Software Requirements
10-31-2017	2.0	Brian McHugh	Finalize

Table of Contents

Purpose

The purpose of the Software Requirements and Architecture document is to develop requirements and metrics against which the item can be verified in order to ensure its functional safety.

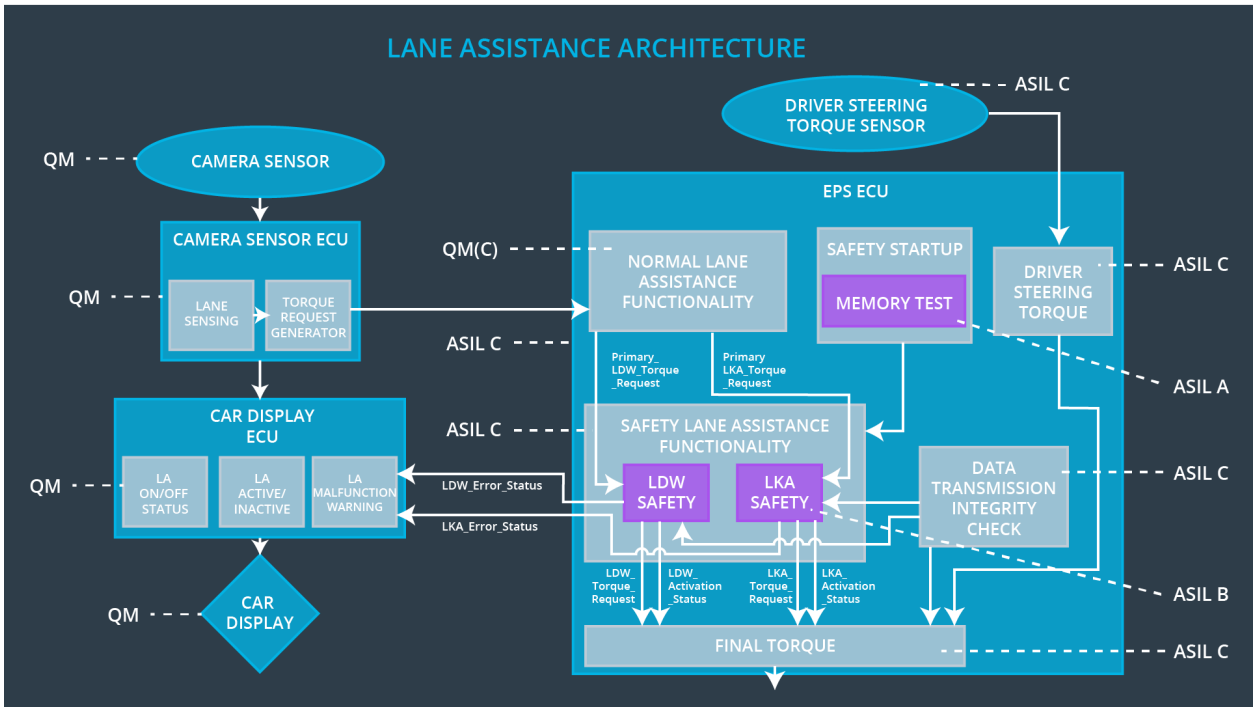
Inputs to the Software Requirements and Architecture Document

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 Safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the Final EPS Torque Generator component does not exceed Max_Torque_Amplitude	C	50 ms	LDW Safety block	LDW torque output is set to 0
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the LDW Safety block shall send a signal to the Car Display ECU to turn on a warning light	C	50 ms	LDW Safety block	LDW torque output is set to 0
Technical Safety Requirement 03	As soon as a failure is detected by the LDW feature, it shall deactivate the LDW function and the LDW_Torque_Request shall be set to 0	C	50 ms	LDW Safety block	LDW torque output is set to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	Data Transmission Integrity Check	LDW torque output is set to 0
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 is set to 0

Refined Architecture Diagram from the Technical Safety Concept



Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

Software Safety Requirements related to Technical Safety Requirement 01:

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 does not exceed Max_Torque_Amplitude	C	50 ms	LDW Safety block	LDW torque output is set to 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 preprocessed to determine the torque request coming from the Normal Lane Assistance Functionality component; processed_LDW_Torq_Req shall be generated at the end of processing	C	LDW_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 01-02	If processed_LDW_Torq_Req has a value greater than Max_Torque_Ampltide_LDW (max allowed safe torque), the torque signal limited_LDW_Torq_Req shall be set to 0, else limited_LDW_Torq_Req shall take the value of processed_LDW_Torq_Req	C	TORQUE_LIMITER	limited_LDW_Torq_Req = 0 (Nm = Newton-meter)
Software Safety Requirement 01-03	limited_LDW_Torq_Req shall be converted into a signal LDW_Torq_Req, which is suitable to be transmitted outside of the LDW Safety component to the Final EPS Torque component. Also see SofSafReq02-01 andSofSafReq02-02	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Request = 0 (Nm)

Software Safety Requirements related to Technical Safety Requirement 02:

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	Data Transmission Integrity Check	N/A

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 with LDW_Torque_Req and activation_status (see SofSafReq03-02) shall be protected by an End2End (E2E) protection mechanism	C	E2ECalc	LDW_Torq_Request = 0 (Nm)
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_Request = 0 (Nm)

Software Safety Requirements related to Technical Safety Requirement 03:

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 0	C	50 ms	LDW Safety	LDW torque output is set to 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	Each of the elements 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 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 (activation_status = 0)	C	LDW_SAFETY_ACTIVATION	activation_status = 0 (LDW function deactivated)
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	N/A
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	C	ALL	LDW_Torq_Request = 0

	that LDW_Torq_Request is set to 0			
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 (LDW function deactivated)

Software Safety Requirements related to Technical Safety Requirement 04:

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 block shall send a signal to the Car Display ECU to turn on a warning light	C	50 ms	LDW Safety block	LDW torque output is set to 0

ID	Software Safety Requirement	ASIL	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 Car Display ECU	C	LDW_SAFETY_ACTIVATION, Car Display ECU	N/A

Software Safety Requirements related to Technical Safety Requirement 05:

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	50 ms	ignition cycle	LDW torque output set to 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	MEMORYTEST	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 (e.g., walking 1's 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 test_status signal	A	MEMORYTEST	activation_status = 0
Software Safety Requirement 05-04	In case any fault is indicated via 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_Request is set to 0	A	MEMORYTEST	activation_status = 0

Refined Architecture Diagram