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
8/25/2018	1.0	Jun Imamura	First Attempt

Table of Contents

Purpose

This document describes requirements for the software components to identify potential probles on SW design and architecture that could lead to a violation of safety goals. These requirements are enough detail to be used for software development.

Inputs to the Software Requirements and Architecture Document

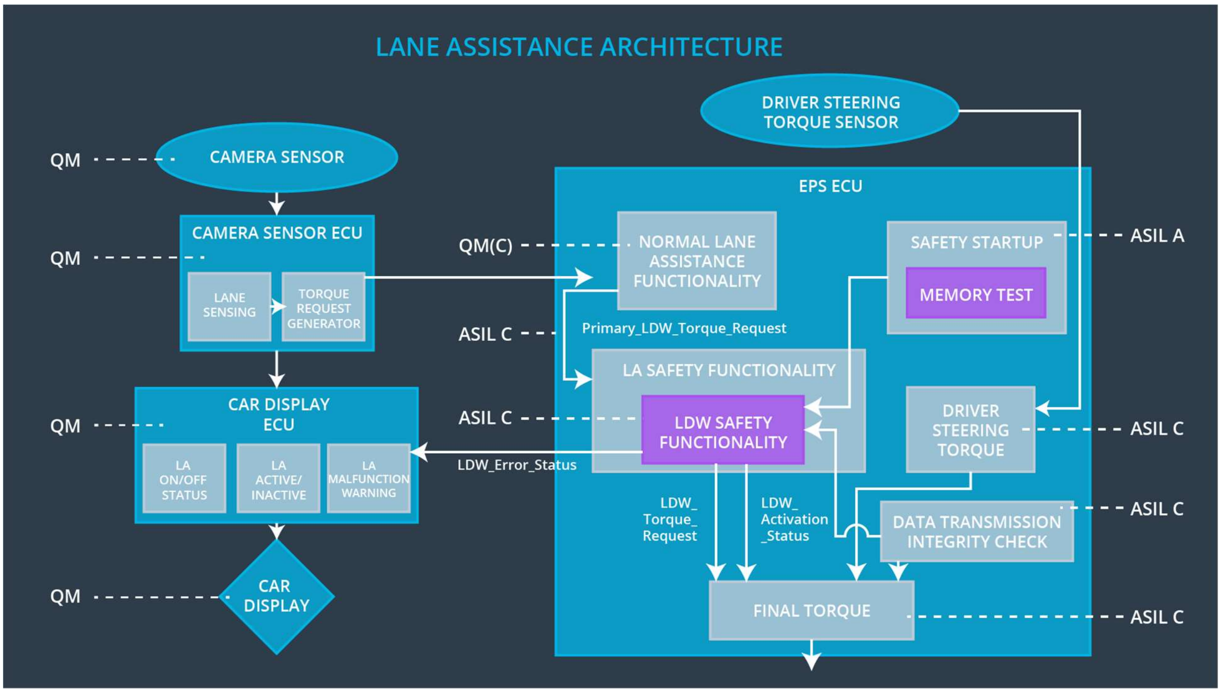
Technical safety requirements

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 that the amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude'	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW Torque Request Amplitude set to zero.
Technical Safety Requirement 01-01-02	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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	
Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, the 'LDW_Torque_Request' shall be set to zero	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	
Technical Safety Requirement	Memory test shall be conducted at start up of the	A	Ignition cycle	Data Transmission Integrity	

01-01-05	EPS ECU to check for any faults in memory.			Check	

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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW Torque Request Amplitude set to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-01-01	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	N/A
Software Safety Requirement 01-01-01-02	In case the “processed_LDW_Torq_Req” signal has a value greater than “Max_Torque_Amplitude_LDW” (maximum allowed safe torque), the torque signal “limited_LDW_Torque_Req” shall be set to 0, else “limited_LDW_Torque_Req” shall take the value of “processed_LDW_Torq_Req”	C	TORQUE_LIMITER	“limited_LDW_Torq_Req” = 0 (Nm=Newton-meter)

Software Safety Requirement 01-01-01-03	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. Also see SofSafReq02-01 and SofSafReq02-02	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 01-02-02	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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW Torque Request Amplitude set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-02-01	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, CarDisplayECU	N/A

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

Technical Safety Requirement 01-02-03	As soon as a failure is detected by the LDW function, the ‘LDW_Torque_Request’ shall be set to zero	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW Torque Request Amplitude set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-03-01	Each of the SW elements shall output a signal to indicate any error which is detected by 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 01-01-03-02	A software element shall evaluate the error status of all the other software elements and in case any 1 of them indicates and error, it 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	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 01-01-03-04	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	LDW_Torq_Req = 0
Software Safety Requirement 03-05	Once the LDW functionality has been deactivated, it shall stay eactivated till the time the ignition is switched from off to on again	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)

ID	Technical Safety Requirement	A	Fault	Allocation to	Safe State

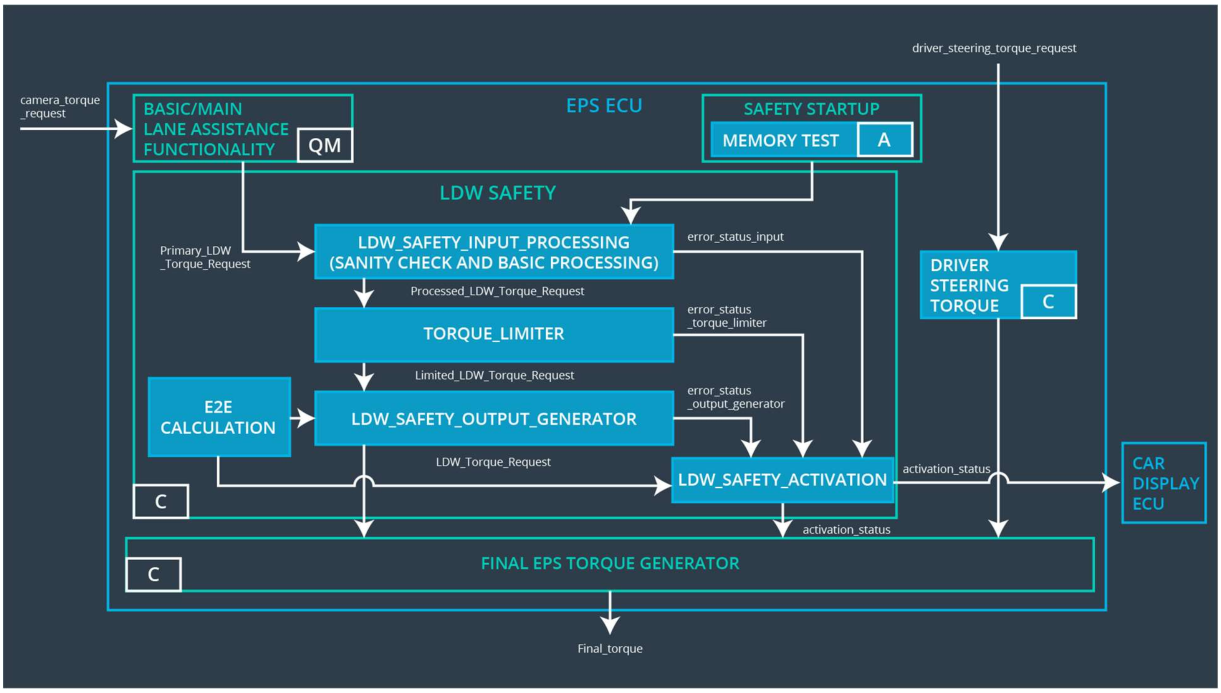
		SIL	Tolerant Time Interval	Architecture	
Technical Safety Requirement 01-02-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	

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 ("LDW Safety") including "LDW_Torque_Req" and "activation_status" (see SofSafReq03-02) shall be protecte by and End2End(E2E) protection mechanism	C	E2ECalc	LDW_Torq_Req = 0(Nm
Software Safety Requirement 01-01-04-01	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(Nm

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	

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-05-01	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 01-01-05-02	Standard RAM tests to check the data bus, address bus and device integrity shall be one every time the ignition is switched from off to on (E.g. walking 1s test, RAM pattern test. Refer RAM and processor vendor recommendations)	A	MEMORYTEST	Activation_status = 0
Software Safety Requirement 01-01-05-03	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 01-01-05-04	In case any fault is indicated via the “test_status” signal the INPUT_LDW_PROCESSING shall sent an error on error_status_input (=1) so that the LDW functionality is deactivated and the LDWTorque is set to 0	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

Refined Architecture Diagram


driver_steering_torque_request
camera_torque_request
EPS ECU
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
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
C
DRIVER STEERING TORQUE
C
CAR DISPLAY ECU
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque