Software Safety Requirements and Architecture

Lane Assistance

Document history

Date	Version	Editor	Description
12/8/2018	1.0	Sindhura Buggaveeti	Initial version

Table of Contents

Purpose

The purpose of the software requirements and architecture document is to develop requirements and metrics against which the iteam can be verified that will ensure its functional saftey

Inputs to the Software Requirements and Architecture Document

[Instructions:

REQUIRED:
You are only required to develop this document for the LDW (lane departure warning) amplitude malfunction. So here, provide the technical safety requirements for the LDW amplitude malfunction as well as the refined system architecture diagram from the technical safety concept.

OPTIONAL:
Expand this document to include software safety requirements for the LDW frequency malfunction as well. Go even further and document software safety requirements for the Lane Keeping Assistance (LKA) function as well.
]

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	C	50ms	LDW safety	LDW torque is set to 0

	'LDW_Torque_Request' sent to the Final electronic power steering Torque component is below 'Max_Torque_Amplitude'				
Technical Safety Requirement 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	LDW safety	LDW torque is set to 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	50ms	LDW safety	LDW torque is set to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request shall be set to zero	C	50ms	Start up	LDW torque 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 the memory	A	50ms	Data transmission integrity check	LDW torque is set to 0

Refined Architecture Diagram from the Technical Safety Concept

[Instructions:

REQUIRED: Provide the refined system 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	LDW safety	LDW torque 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 pre-processed to determine the torque request coming from the "Basic/Main LA Functionality" SW component. Signal	C	LDW_SAFETY_INPUT_PROCESSING	N/A

	"processed_LDW_Torq_Req" shall be generated at the end of the processing			
Software Safety Requirement 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_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	The limited_LDW_Torq_Req shall be transformed to "LDW_Torq_Req" which is suitable to be transmitted outside of LDW safety component to the "Final EPS Torque" component. Also see SofSafReq02-01 and SofSafReq02-02	C	LDW_SAFETY_OUTPUT _GENERATOR	LDW_Torq_Req =0(Nm=Newton-meter)

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	50ms	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 ("LDW Safety") including "LDW_Torque_Req" and "activation_status" (see SofSafReq03-02) shall be protected by an End2End(E2E)	C	E2ECalc	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 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 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	50ms	LDW Safety	LDW torque is set to 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(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 incase 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 that "LDW_Torq_Req" is set to 0	C	All	LDW_Torq_Req=0

Software Safety Requirement 03-05	Once 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)

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	50ms	LDW Safety	LDW torque 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 the car display ECU	C	LDW_SAFETY_ACTIVATION, CarDisplay 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	Memory Test	LDW torque is 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 swicthed from off to on	A	MEMORYTEST	Activation_status=0
Software Safety Requirement 05-03	The test result of the RAM or Flash memeory 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 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