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
9/1/2017	1.0	Flora Sun	Initial Draft

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Purpose

This document describe functional safety requirements includes specific rules on how to implement hardware and software.

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 Electronic Power Steering Torque' component is below 'Max_Torque_Amplitude	C	50ms	LDW Safety Software component	The LDW Torque output is set to zero.
Technical Safety Requirement	The validity and integrity of the data transmission for	C	50ms	Data Transmission Integrity	N/A

02	'LDW_Torque_Request' signal shall be ensured.			Check	
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 Software component	The LDW Torque output is set to zero.
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 Software component	The LDW Torque output is set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Length of Ignition Cycle	Memory Test Block	The LDW Torque output is set to zero.

Refined Architecture Diagram from the Technical Safety Concept

[Instructions: REQUIRED: Provide the refined system architecture diagram from the technical safety concept]
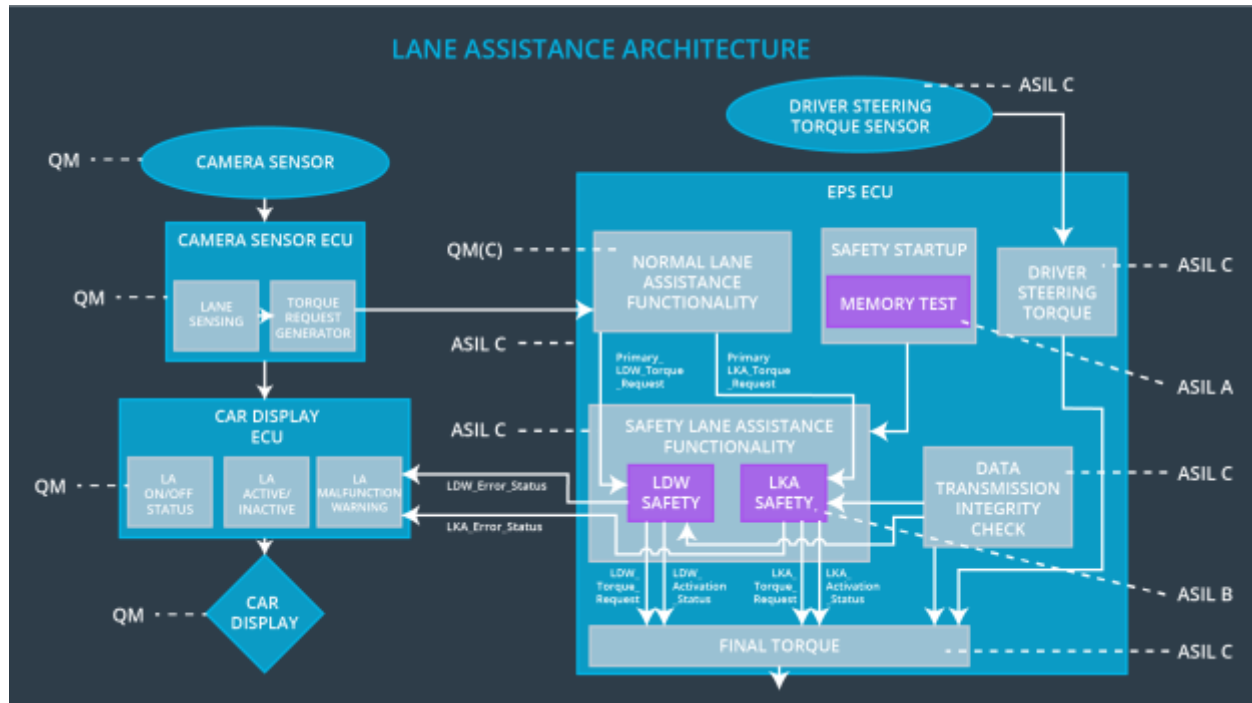
Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

[Instructions: Fill in the software safety requirements for the LDW amplitude malfunction technical safety requirements. We have provided the associated technical safety requirements. Hint: The software safety requirements were discussed in the text from the software and hardware lesson.

OPTIONAL:

CHALLENGE ONE
Develop software safety requirements for the Lane Departure Warning (LDW) frequency function and modify the system architecture as needed.

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 software component | The LDW Torque output is set to zero. |

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01	The input signal Primary_LDW_Torque_Request shall be read and pre-processed to determine the torque request coming from the Basic/Main Lane Assistance Functionality SW Component. Signal Processed_LDW_Torque_Request shall be generated at the end of the processing.	C	LDW_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 01-02	In case the Processed_LDW_Torque_Request signal has a value greater than Max_Torque_Ampltide_LDW (the maximum allowed safe torque), the torque signal Limited_LDW_Torque_Request shall be set to 0, else Limited_LDW_Torque_Request shall take the value of	C	TORQUE_LIMITER	Limited_LDW_Torque_Request" = 0 (Nm=Newton-meter)

	Processed_LDW_Torque_Request.			
Software Safety Requireme nt 01-03	The Limited_LDW_Torque_Reque st shall be transformed into a signal LDW_Torque_Request which is suitable to be transmitted outside of the LDW Safety component ("LDW Safety") to the "Final EPS Torque" component." Also see SofSafReq02-01 andSofSafReq02-02	C	LDW_SAFETY_OUTPU T_GENERATOR	LDW_Torque_ Request = 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.	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_Request" and "activation_status" (seeSofSafReq03-02) shall be protected by an End2End(E2E) protection mechanism.	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 Software component	The LDW Torque output is set to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement03-01	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 Requirement03-02	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	In case of no errors from the software elements, the status	C	LDW_SAFETY_ACTIVATIO	N/A

Requirement03-03	of the LDW feature shall be set to activated ("activation_status" = 1)		N	
Software Safety Requirement03-04	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_Torque_Request" is set to 0.	C	All	LDW_Torq_Req = 0
Software Safety Requirement03-05	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)

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 Software component	The LDW Torque output is set to zero.

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	A S I L	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	Length of ignition cycel	Memory Test Block	The LDW Torque output is set to zero.

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requireme nt 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 Requireme nt 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 1s test, RAM pattern test. Refer RAM and processor vendor recommendations)	A	MEMORYTEST	Activation_status = 0
Software Safety Requireme nt 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	In case any fault is indicated via the "test_status" signal	A	LDW_SAFETY_ INPUT_PROCE	Activation_status = 0

| Requirement 05-04 | 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 | | SSING | |

Refined Architecture Diagram

[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the software and hardware lesson, including all of the ASIL labels.]