Software Safety Requirements and Architecture

Lane Assistance

Document Version: 1.2

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
Apr. 1, 2018	1.1	Yi-Ching Chung	First draft from template
APr. 3, 2018	1.2	Yi-Ching Chung	Second draft with revisions

Table of Contents

Purpose

This document intends to identify the new requirements for the software components at a component level in order to identify potential problems on software design and architecture that could lead to a violation of safety goals. These requirements are more detail oriented than the technical safety concept requirements.

Inputs to the Software Requirements and Architecture Document

Technical safety requirements

Table 1 provide the technical safety requirements for the LDW amplitude malfunction as well as the refined system architecture diagram from the technical safety concept.

Table 1 Technical Safety Requirements related to Functional Safety Requirement 01-01

ID	**Technical Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Architecture Allocation**	**Safe State**
Technical Safety Requirement 01	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 Block	The lane departure warning torque request amplitude shall be set to zero.
Technical Safety Requirement 02	Validity and Integrity of the data transmission for the LDW_Torque_Request signal shall be ensured	C	50 ms	Data Transmission Integrity Check	The lane departure warning torque request amplitude shall be set

					to zero.
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 Block	The lane departure warning torque request amplitude shall be 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	50 ms	LDW Safety Block	The lane departure warning torque request amplitude shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at the startup of EPS ECU to check for any faults in memory.	A	Ignition cycle	Separate External block with Memory test code	The lane departure warning torque request amplitude shall be set to zero.

Refined Architecture Diagram from the Technical Safety Concept

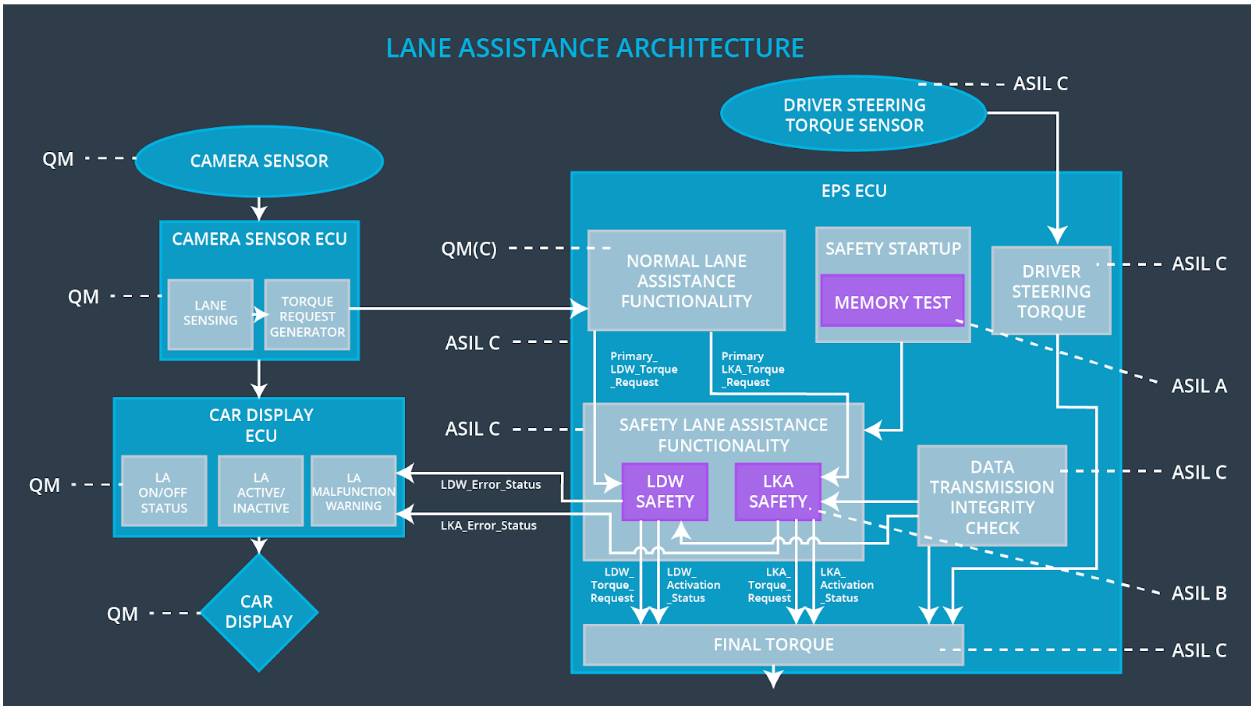

Fig. 1 refined system architecture diagram from the technical safety concept

Software Requirements

The Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements are listed in Table 2 and Table 3.

Table 2 Software safety requirements for the LDW amplitude malfunction technical safety requirement 01.

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent	C	50 ms	LDW Safety Block	The lane departure warning torque request

01	to the Final Electronic Power Steering Torque component is below Max_Torque_Amplitude				amplitude shall be set to zero

Table 3 Detailed Software safety requirements for the LDW amplitude malfunction technical safety requirements 01.

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 LAFunctionality’ SW Component. Signal ‘processed_LDW_Torq_Req’ shall be generated at the end of the processing.	C	LDW_SAGETY_INPUT_PROCESSING	N/A
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 zero, 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 into a signal ‘LDW_Torq_Req’ which is suitable to be transmitted outside the LDW	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

	Safety component (‘LDW Safety’) to the ‘Final EPS Torque’ component.			

Table 4 Software safety requirements for the LDW amplitude malfunction 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	The lane departure warning torque request amplitude shall be set to zero

Table 5 Detailed Software safety requirements for the LDW amplitude malfunction technical safety requirements 02.

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” (seeSofSafReq03-02) shall be protected by an End2End(E2E)protection mechanism	C	E2C Calc	LDW_Torq_Req = 0 (Nm)
Software Safety Requirement 02-02	The E2E protection protocol shall contain and attach the control data: alive counter	C	E2E Calc	LDW_Torq_Req = 0 (Nm)

	(SQC) and CRC to the data to be transmitted			

Table 6 Software safety requirements for the LDW amplitude malfunction 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 zero	C	50 ms	LDW Safety	LDW torque output is set to zero

Table 7 Detailed Software safety requirements for the LDW amplitude malfunction technical safety requirements 03.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement03-01	Each Software element shall output a 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 other software elements and in case any one of them indicates an error, it shall	C	LDW_SAFETY_ACTIVATION	Lane Departure Warning function deactivated ('activation_status' =0).

	deactivate the Lane Departure Warning feature (‘activation_status’=0)			
Software Safety Requirement03-03	In case of a no error from the software elements, the status of the Lane Departure Warning feature shall be set to activated (‘activation_status’=1).	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement03-04	In case an error is detected by any of the software elements, it shall set the value to its corresponding torque to zero so that ‘LDW_Torq_Req’ is set to zero	C	All	LDW_Torq_Req = 0
Software Safety Requirement03-05	Once the Lane Departure Warning functionality has been deactivated, it shall stay deactivating until the time the ignition is switched from off to on again.	C	LDW_SAFETY_ACTIVATION	Lane Departure Warning function deactivated (‘activation_status’ =0).

Table 8 Software safety requirements for the LDW amplitude malfunction 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 software 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 zero

Table 9 Detailed Software safety requirements for the LDW amplitude malfunction technical safety requirements 04.

ID	**Software Safety**	**AS**	**Allocation Software**	**Safe State**

	Requirement	IL	Elements	
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

Table 10 Software safety requirements for the LDW amplitude malfunction 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	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque output is set to zero.

Table 11 Detailed Software safety requirements for the LDW amplitude malfunction technical safety requirements 05.

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 content corruption.	A	MEMORYTEST	Activation_status = 0
Software Safety	Standard RAM test to check the data bus, address bus	A	MEMORYTE	Activation_status = 0

Requirement 05-02	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)		ST	
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

The refined system architecture should include the system architecture from the end of the software and hardware lesson, including all of the ASIL labels (in Fig. 2).

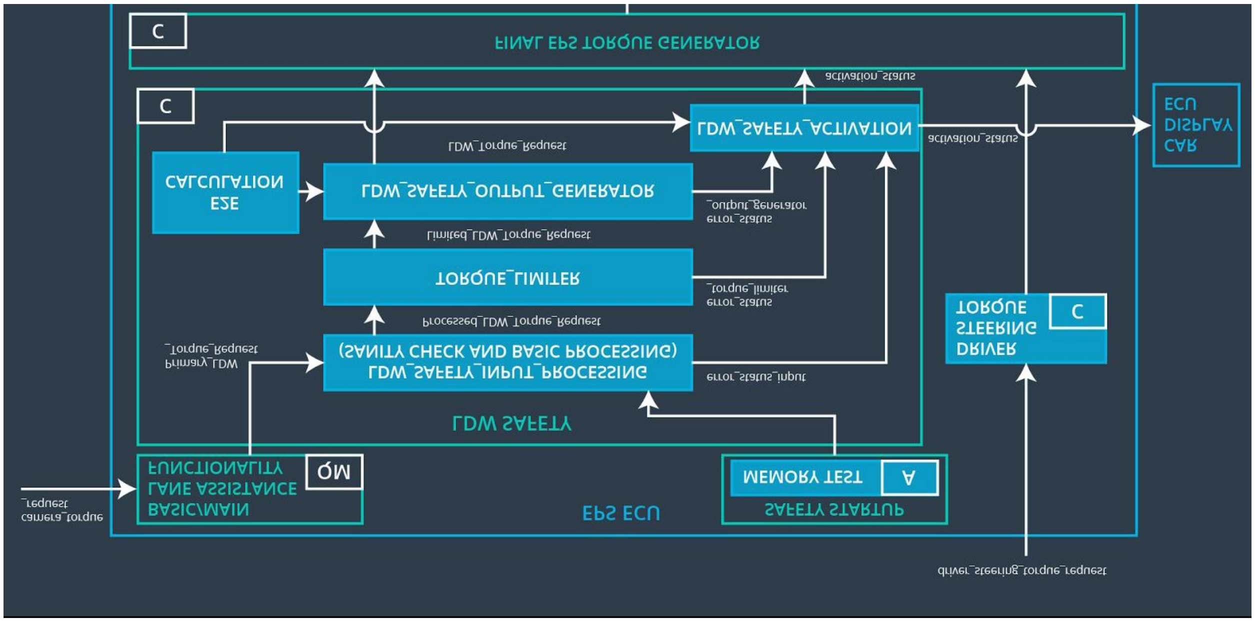

Fig. 2 Refined system architecture.