Software Safety Requirements and Architecture

Lane Assistance

Document Version: [Version]1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
06/15/2018	1.0	Efraim Kropp	Initial version

Table of Contents

1. Purpose

The purpose of this document is to define software requirements and the software architecture that will ensure functional safety of the Lane Assistance item.

2. Inputs to the Software Requirements and Architecture Document

2.1. 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	50 ms	LDW Safety component	LDW torque output is set to zero

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	LDW torque output is 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 component	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	50 ms	LDW Safety component	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	Ignition cycle	Memory test	LDW torque output is set to zero

2.2. Refined Architecture Diagram from the Technical Safety Concept

[Instructions:

REQUIRED: Provide the refined system architecture diagram from the technical safety concept
]
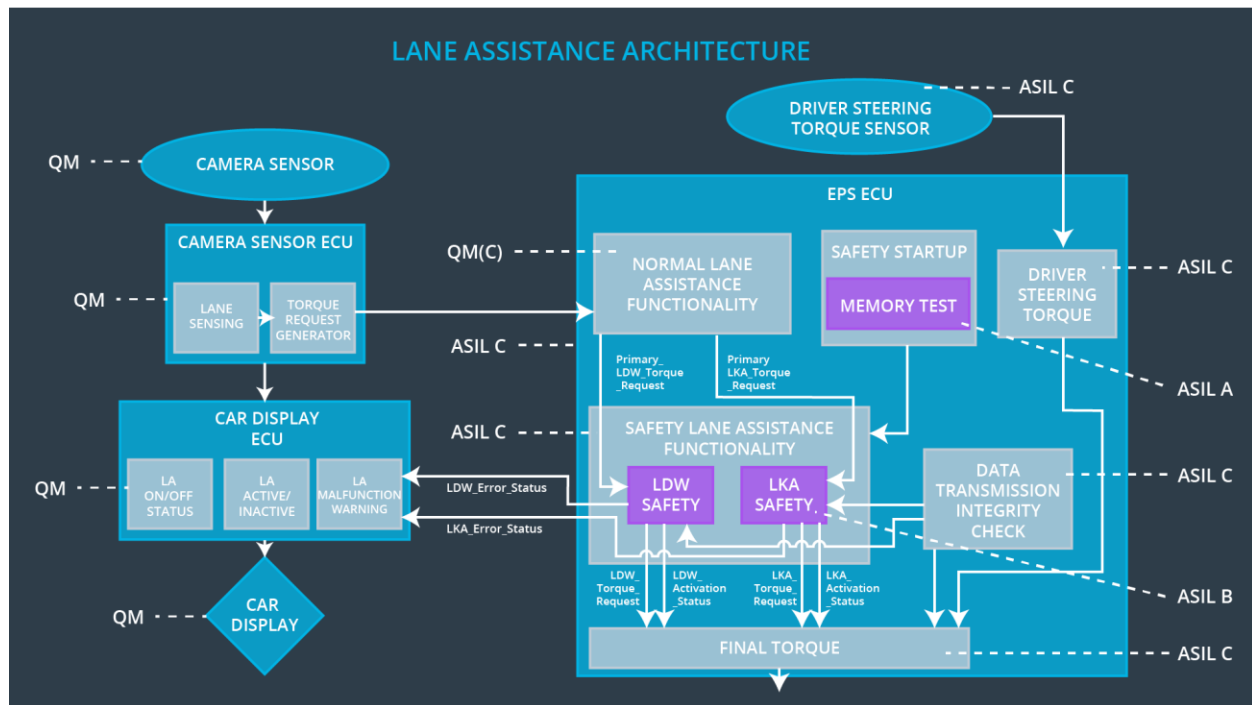
Figure 1 Refined Architecture Diagram from the Technical Safety Concept

3. Software Requirements

3.1. 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	50 ms	LDW Safety component	LDW torque output is set to zero

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software	The input signal	C	LDW_SAFETY_INPUT_P	"error_status_in

Safety Requirement 01-01	"Primary_LDW_Torque_Request" shall be read and pre-processed to determine the torque request coming from the "Basic/Main LA Functionality" SW Component. Signal "Processed_LDW_Torque_Request" shall be generated at the end of the processing.		ROCESSING (SANITY CHECK AND BASIC PROCESSING)	put" is set to "error"
Software Safety Requirement 01-02	In case the "Processed_LDW_Torque_Request" signal has a value greater than "Max_Torque_Amplitude" (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 "Processed_LDW_Torque_Request"	C	TORQUE_LIMITER	"Limited_LDW_Torque_Request" is set to 0 "error_status_torque_limiter" is set to "error"
Software Safety Requirement 01-03	The "Limited_LDW_Torque_Request" 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 Generator" component. Also see Software Safety Requirements 02-01 and 02-02	C	LDW_SAFETY_OUTPUT _GENERATOR	"LDW_Torque_Request" is set to 0. "error_status_output_generator" is set to "error"

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	LDW torque output is set to zero

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 including "LDW_Torque_Request" and "activation_status" (see Software Safety Requirement 03-02) shall be protected by E2E protection mechanism	C	E2E CALCULATION	"LDW_Torque_Request" is set to 0. "activation_status" is set to "inactive"
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	E2E CALCULATION	N/A

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

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_generator(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 is 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_Torque_Request" is	C	All	"LDW_Torque_Request" is set to 0

	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 is 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	50 ms	LDW Safety	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	CAR DISPLAY ECU, LDW_SAFETY_ACTIVATION	"activation_status" = 0 (LDW function is deactivated)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	A	Ignition cycle	MEMORY TEST	LDW torque output is set to zero

| 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	MEMORY TEST	"activation_status" = 0 (LDW function is deactivated)
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	A	MEMORY TEST	"activation_status" = 0 (LDW function is deactivated)
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	MEMORY TEST	"activation_status" = 0 (LDW function is deactivated)
Software Safety Requirement 05-04	In case any fault is indicated via the "test_status" signal the LDW_SAFETY_INPUT_PROCESSING block 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	MEMORY TEST	"activation_status" = 0 (LDW function is deactivated)

4. Refined Architecture Diagram
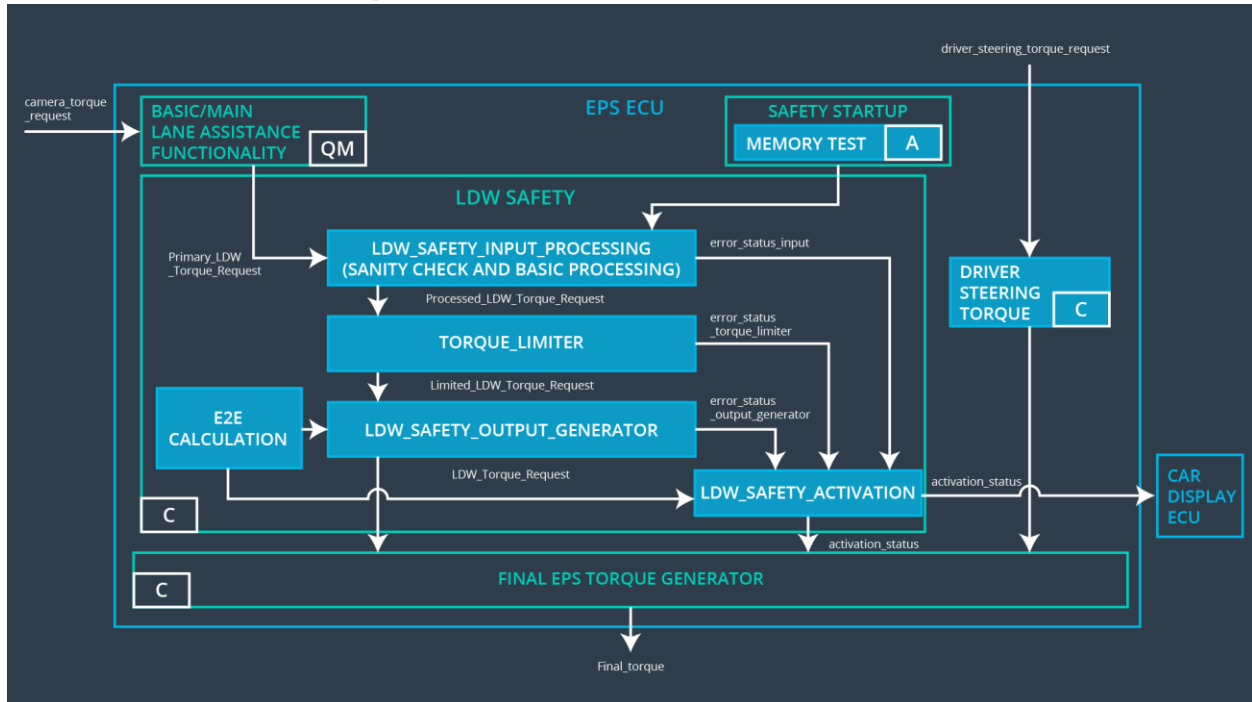
Figure 2 Refined Architecture Diagram