Software Safety Requirements and Architecture Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12-27-2018	1.0	Nick Fiege	

Table of Contents

Purpose

The purpose of this document is to identify requirements for the system at software component level based on the technical safety requirements specified in earlier documents.

Requierements defined in here will be more specific to details of the actual software module implementation.

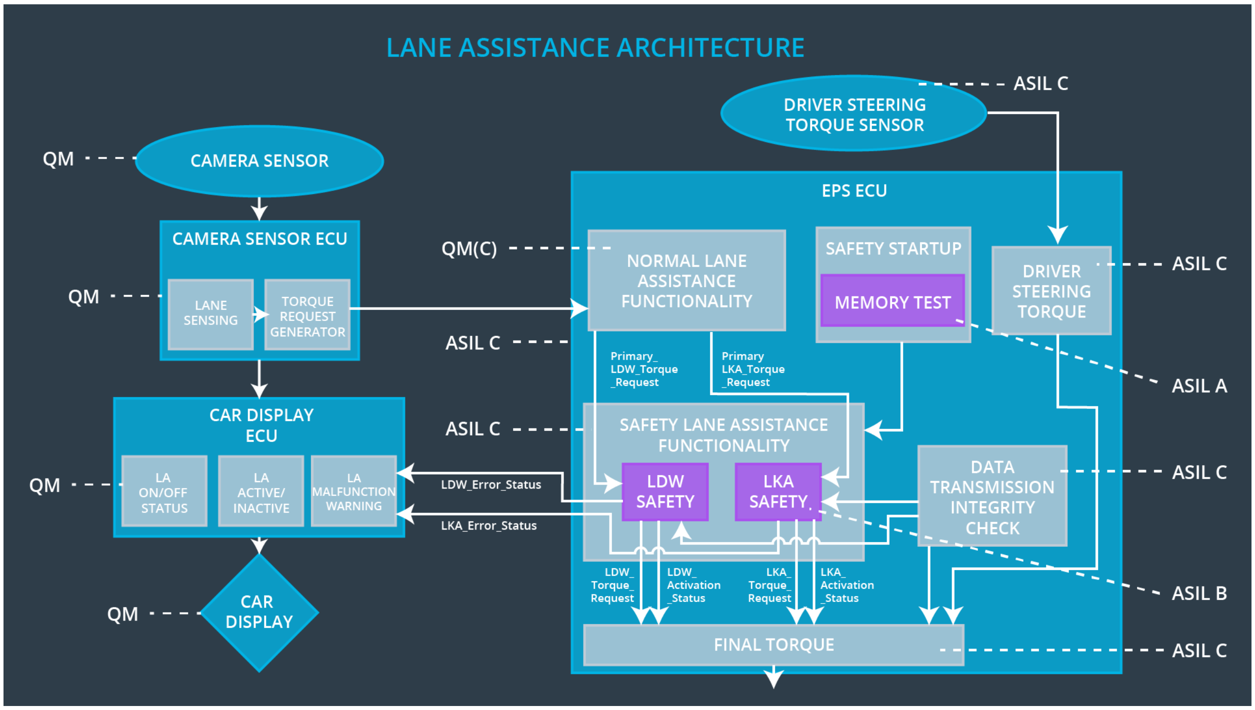
Inputs to the Software Requirements and Architecture Document

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	50 ms	LDW Safety	LDW sets torque request to zero.
Technical Safety Requirement 02	On deactivation of the LDW function, the LDW Safety shall send a signal to the display ECU to turn on a warning indicator.	C	50 ms	LDW safety	LDW sets torque request to zero.
Technical Safety Requirement 03	On error detection, the LDW safety shall deactivate the LDW function and the requested torque shall be set to zero.	C	50 ms	LDW safety	LDW sets torque request to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for torque request signals shall be ensured.	C	50 ms	LDW safety	LDW sets torque request to zero.
Technical Safety Requirement 05	A initialization memory test routine shall be conducted at start up of the EPS ECU to check for any faults in memory.	B	Initialization/Ignition cycle	Data transmission integrity check	LDW sets torque request to zero.

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	50 ms	LDW Safety	LDW sets torque request to zero.

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 stored to determine the torque request coming from the Normal Lane Assistance Functionality. The buffered input signal shall be named ‘Processed_LDW_Torq_Req’.	C	LDW_SAFETY_INPUT_PROCESSING	Processed_Torque_request = 0
Software Safety Requirement 01-02	In case the’ processed_torque_request’ signal has a greater value than “max_torque_amplitude_LDW” the 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
Software Safety Requirement 01-03	The signal ‘Limited_LDW_Torq_Req’ shall be processed into ‘LDW_Torq_Req’ which is suitable to be received by the ‘Final Torque’ component.	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02	On deactivation of the LDW function, the LDW Safety shall send a signal to the display ECU to turn on a warning indicator.	C	50 ms	LDW safety	LDW sets torque request to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 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’ -> ‘CAR DISPLAY ECU’	None

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 03	On error detection, the LDW safety shall deactivate the LDW function and the requested torque shall be set to zero.	C	50 ms	LDW safety	LDW sets torque request to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	Every element shall generate a signal to indicate errors with it's own execution. 'LDW_SAFETY_INPUT_PROCESSING' shall therefore generate the 'error_status_input' signal. 'TORQUE_LIMITER' shall therefore generate the 'error_status_torque_limiter' signal 'LDW_SAFETY_OUTPUT_GENERATOR' shall therefore generate the 'error_status_output_gen' signal.	C	'LDW_SAFETY_INPUT_PROCESSING' 'TORQUE_LIMITER', 'LDW_SAFETY_OUTPUT_GENERATOR' -> 'LDW_SAFETY_ACTIVATION'	None
Software Safety Requirement 03-02	A software element shall evaluate all of the error signals and indicates an error if any '1' is received. It shall deactivate the LDW feature by setting the 'activation_status' to '0' and therefore dactivate the LDW functionality.	C	LDW_SAFETY_ACTIVATION	'activation_status' = 0
Software Safety Requirement 03-03	When no errors are detected, the status of the LDW feature shall be activated by setting 'activation_status' to '1'.	C	LDW_SAFETY_ACTIVATION	None
Software Safety Requirement 03-04	Once the LDW functionality has been deactivated, it shall stay deactivated until the ignition is switched from off to on again.	C	LDW_SAFETY_ACTIVATION	'activation_status' = 0

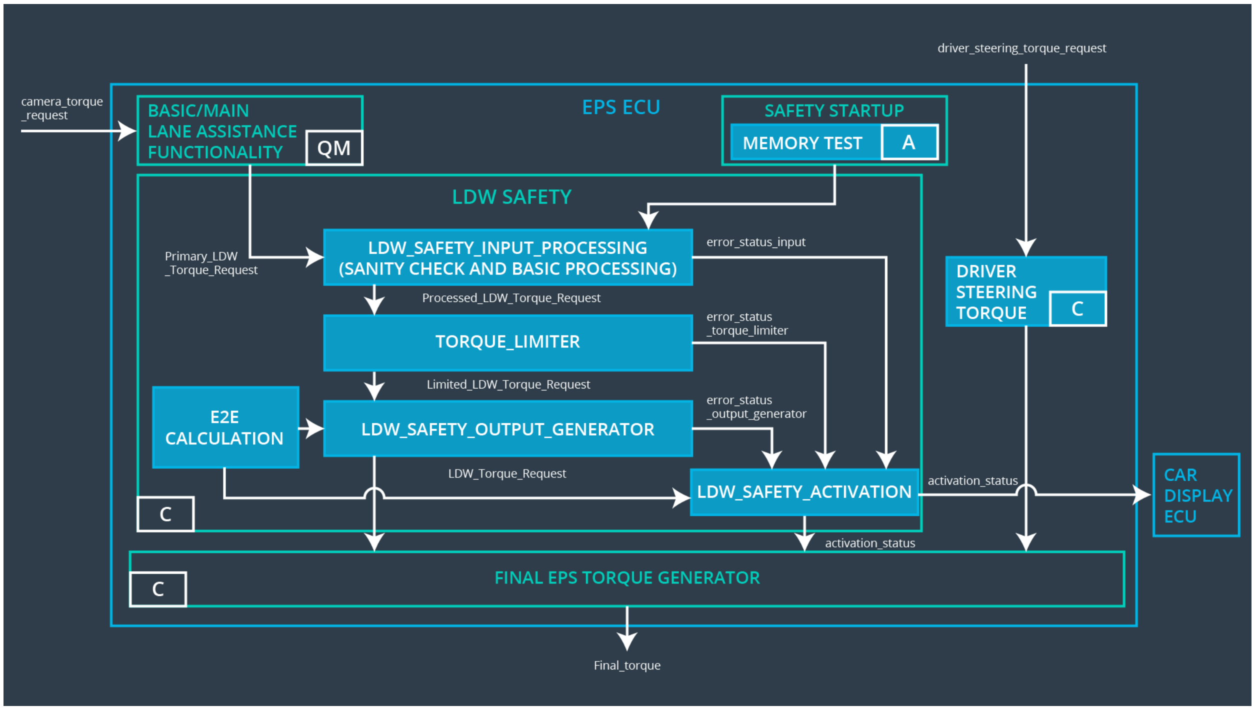
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 04	The validity and integrity of the data transmission for torque request signals shall be ensured.	C	50 ms	LDW safety	LDW sets torque request to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	Data transmitted from/to the 'LDW_Safety_Activation' component and the 'LDW_SAFETY_OUTPUT_GENERATOR' shall be protected by an end to end(E2E) protection mechanism	C	E2ECalc	'LDW_Torq_Req' = 0
Software Safety Requirement 04-02	The E2E protection protocol shall contain protection data like an alive counter (SQC) and CRC of the data transmitted.	C	E2ECalc	'LDW_Torq_Req' = 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	A initialization memory test routine shall be conducted at start up of the EPS ECU to check for any faults in memory.	B	Initialization/Ignition cycle	Data transmission integrity check	LDW sets torque request to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 05-01	On each system initialization(ignition), a CRC verification check of source code inside the flash memory shall be done.	A	MEMORYTEST	‘activation_status’ = 0
Software Safety Requirement 05-02	Tests to check RAM, address/data bus and device integrity shall be done on each system initialization(ignition).	A	MEMORYTEST	‘activation_status’ = 0
Software Safety Requirement 05-03	The test result of the RAM or Flash memory shall be indicated to the LDW_Safety component via the memory_status” signal	A	MEMORYTEST	‘activation_status’ = 0
Software Safety Requirement 05-04	A negative (0) ‘memory_status” signal in the ‘INPUT_LDW_PROCESSING’ component shall set the signal ‘error_status_input’ to ‘1’, so that the LDW functionality is deactivated safely.	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
FINAL EPS TORQUE GENERATOR
C
Final_torque