



# Software Safety Requirements and Architecture

## Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



# Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
23-May-18	1	Arpit Srivastava	Version 1

## Table of Contents

[Document history](#)

[Table of Contents](#)

[Purpose](#)

[Inputs to the Software Requirements and Architecture Document](#)

[Technical safety requirements](#)

[Refined Architecture Diagram from the Technical Safety Concept](#)

[Software Requirements](#)

[Refined Architecture Diagram](#)

# Purpose

This document is a more detail oriented reference for identifying potential problems in software and hardware design that may lead to violations of safety requirements.

## Inputs to the Software Requirements and Architecture Document

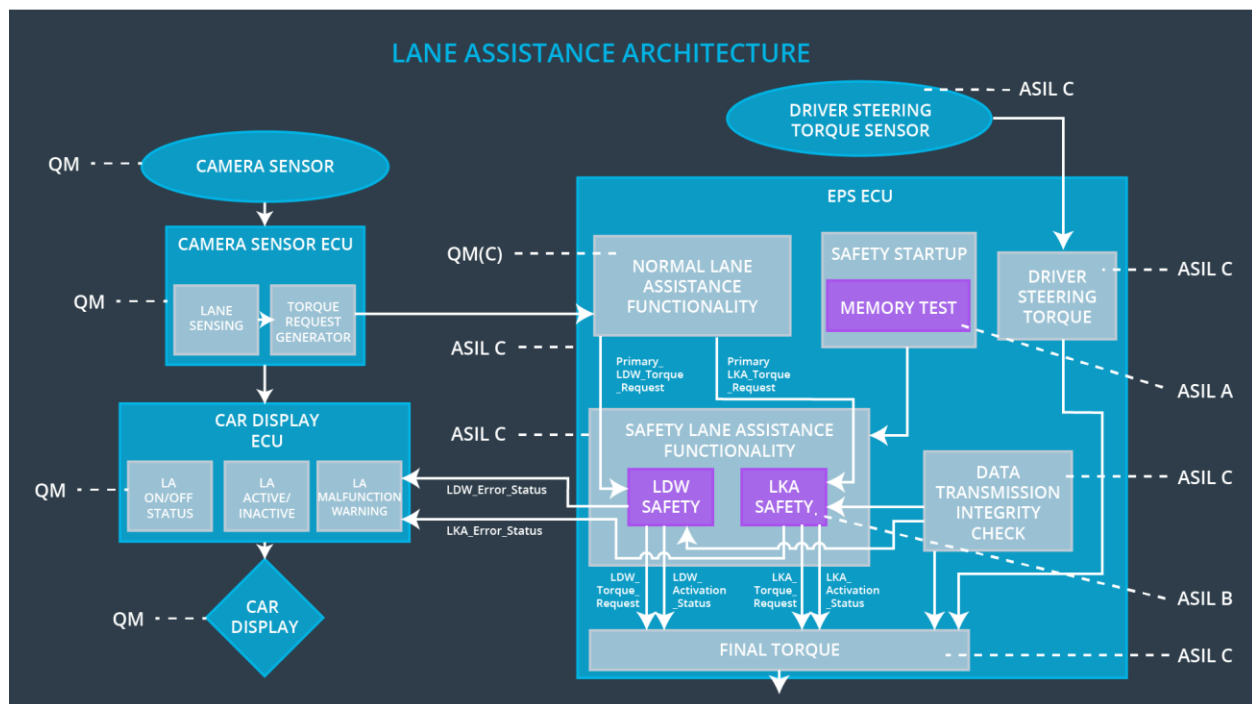
### Technical safety requirements

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 01-01-01	The Lane Departure Warning 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	Lane Departure
Technical Safety Requirement 01-01-02	When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 01-01-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.
Technical	The validity and integrity of	C	50 ms	LDW Safety	Lane

Safety Requirement 01-01-04	the data transmission for 'LDW_Torque_Request' signal shall be ensured.				Departure Warning torque to zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

## Refined Architecture Diagram from the Technical Safety Concept



# Software Requirements

## Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

ID	Technical Safety Requirement	A S I L	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-01	The Lane Departure Warning 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	Lane Departure Warning torque to zero.

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-01-01	The input signal 'Primary_LDW_Torq_Req' shall be read and pre-processed to determine the torque request coming from the 'Basic/Main LAF functionality' SW Component. Signal 'processed_LDW_Torq_Req' shall be generated at the end of the processing.	C	LDW_SAGETY_INPUT_P ROCESSING	N/A
Software Safety Requirement 01-01-01-02	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	C	TORQUE_LIMITER	'limited_LDW_Torq_Req' = 0 (Nm=Newton-meter)

	take the value of 'processed_LDW_Torq_Req'			
Software Safety Requirement 01-01-01-03	The 'limited_LDW_Torq_Req' shall be transformed into a signal 'LDW_Torq_Req' which is suitable to be transmitted outside the LDW Safety component ('LDW Safety') to the 'Final EPS Torque' component.	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-02	When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-02-01	Any data to be transmitted outside the LDQ Safety component ('LDW Safety') including 'LDW_Torque_Req' and 'activation_status' shall be protected by an End-2-End protection mechanism.	C	E2C Calc	LDW_Torq_Req = 0 (Nm)
Software Safety Requirement 01-01-02-02	The E2E protection protocol shall contain and attach the control data (alive counter (SQC) and CRC) to the data to be transmitted.	C	E2E Calc	LDW_Torq_Req = 0 (Nm)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-03-01	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 Requirement 01-01-03-02	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 deactivate the Lane Departure Warning feature ('activation_status'=0)	C	LDW_SAFETY_ACTIVATION	Lane Departure Warning function deactivated ('activation_status' =0).
Software Safety Requirement 01-01-03-03	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	In case an error is detected by any of the software elements, it	C	All	LDW_Torq_Req = 0



Requirement 01-01-03-04	shall set the value to its corresponding torque to zero so that 'LDW_Torq_Req' is set to zero			
Software Safety Requirement 01-01-03-05	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).

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-04-01	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

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 01-01-05-01	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	MEMORYTES T	Activation_status = 0
Software Safety Requirement 01-01-05-02	Standard RAM test 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 to RAM and processor vendor recommendations)	A	MEMORYTES T	Activation_status = 0
Software Safety Requirement 01-01-05-03	The test result of the RAM or Flash memory shall be indicated to the LDW_Safety component via the 'test_status' signal.	A	MEMORYTES T	Activation_status = 0
Software Safety Requirement 01-01-05-04	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_PRO CESSING	Activation_status = 0

# Refined Architecture Diagram

