



# 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
2018-03-04	1.0	Maximilian Wenger	Initial version

## Table of Contents

Document history .....	2
Table of Contents.....	2
Purpose .....	3
Inputs to the Software Requirements and Architecture Document.....	3
Technical safety requirements .....	3
Refined Architecture Diagram from the Technical Safety Concept.....	4
Software Requirements.....	5
Refined Architecture Diagram .....	12

# Purpose

The purpose of this document is to document the software safety requirements for the lane assistance item. Specifically, it focuses on the LDW (lane departure warning) amplitude malfunction.

## Inputs to the Software Requirements and Architecture Document

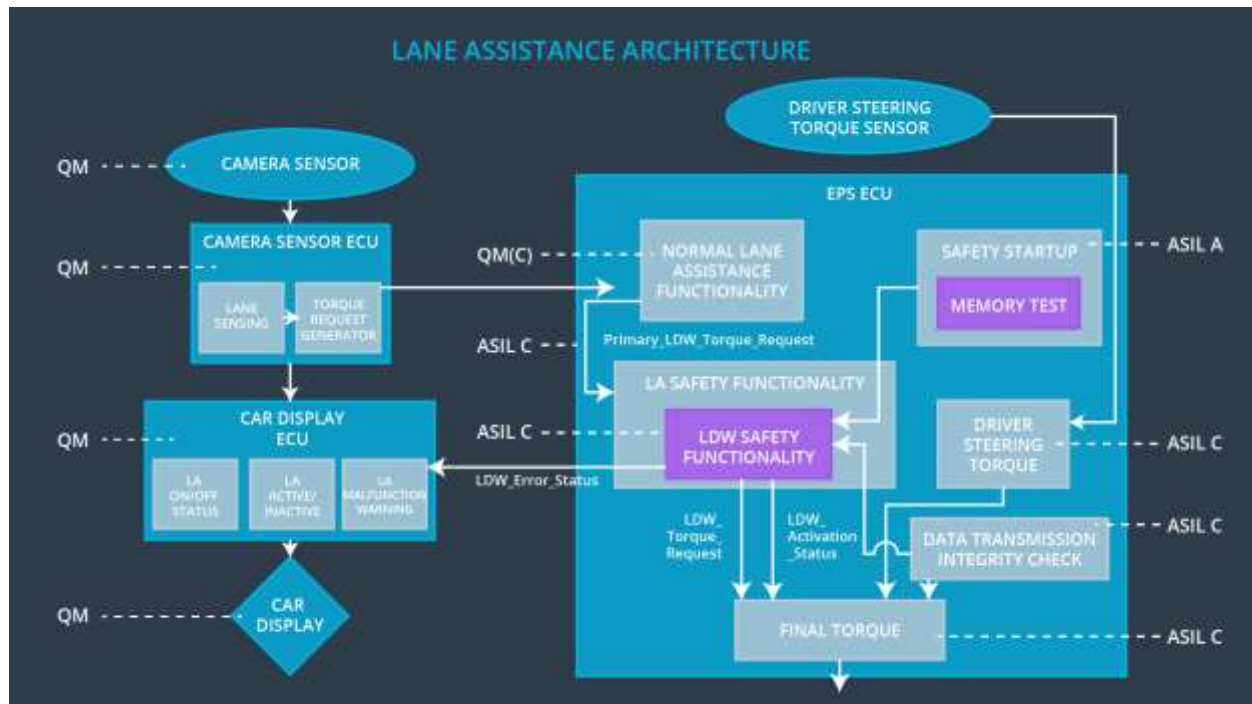
### Technical safety requirements

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 functionality	LA off (torque zero)
Technical Safety Requirement 02	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 functionality	LA off (torque 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 functionality	LA off (torque zero)
Technical Safety Requirement	The validity and integrity of the data transmission for 'LDW_Torque_Request' sig-	C	50 ms	Data Transmission Integrity Check	LA off (torque zero)

04	nal shall be ensured.				
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	Memory Test	LA off (torque 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 In- terval	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 functionality	LA off (torque zero)

ID	Software Safety Requirement	A S I L	Allocation Software El- ements	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 LAF functionality" SW Component. Signal "processed_LDW_Torq_Req" shall be generated at the end of the processing.	C	LDW_SAFETY_INPUT_P ROCESSING	N/A
Software Safety Re- quirement 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 0, 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 of the LDW Safety component ("LDW Safety") to the "Final EPS Torque" component. Also see Software Safety Requirement 02-01 and Software Safety Requirement 02-02	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)
-----------------------------------	---	---	-----------------------------	-----------------------

ID	Technical Safety Requirement	A S I L	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	LDW Safety functionality	LA off (torque zero)

ID	Software Safety Requirement	A S I L	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" (see Software Safety Requirement 03-02) 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	A S I L	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 functionality	LA off (torque zero)

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Re- quire- ment03-01	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 Re- quire- ment03-02	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 Re- quire- ment03-03	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 Re-	In case an error is detected by any of the software elements, it shall	C	All	LDW_Torq_Req = 0



quire- ment03-04	set the value of its corresponding torque to 0 so that "LDW_Torq_Req" is set to 0			
Software Safety Re- quire- ment03-05	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_ AC- TIVATION	Activation_status = 0 (LDW function deactivated)

ID	Technical Safety Requirement	A S I L	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	Data Transmis- sion Integrity Check	LA off (torque ze- ro)

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Re- quirement 04-01	When the LDW function is deac- tivated (activation_status set to 0), the activation_status shall be sent to the car displayECU.	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	Ignition cycle	Memory Test	LA off (torque zero)

ID	Software Safety Requirement	A S I L	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	MEMORYTEST	Activation_status = 0
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 (E.g. walking 1s test, RAM pattern test. Refer RAM and processor vendor recommendations )	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 "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 error_status_input (=1) so that the LDW functionality is deactivated and the LDWTorque is set to 0	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

The diagram illustrates the functional blocks and data flow within the EPS ECU for LDW safety:

- Inputs:**
  - Camera torque request** (External input to BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY)
  - driver steering torque request** (External input to DRIVER STEERING TORQUE)
- Internal Blocks and Flow:**
  - BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY (QM)** receives the camera torque request and outputs **Primary LDW Torque Request** to **LDW SAFETY INPUT PROCESSING (SANITY CHECK AND BASIC PROCESSING)**.
  - SAFETY STARTUP MEMORY TEST (A)** provides an **error\_status\_input** to the **LDW SAFETY** block.
  - LDW SAFETY** is a central processing block that receives the primary request and error status input. It outputs a **Processed LDW Torque Request** to the **TORQUE LIMITER**.
  - TORQUE LIMITER** outputs a **Limited LDW Torque Request** to the **LDW SAFETY OUTPUT GENERATOR**.
  - E2E CALCULATION (C)** receives the primary request and provides an input to the **LDW SAFETY OUTPUT GENERATOR**.
  - LDW SAFETY OUTPUT GENERATOR** outputs an **LDW Torque Request** to the **LDW SAFETY ACTIVATION** block and also provides an **error\_status\_output\_generator** input to it.
  - LDW SAFETY ACTIVATION** receives the limited request, the output generator input, and the **error\_status\_input**. It outputs an **activation\_status** to the **FINAL EPS TORQUE GENERATOR**.
  - DRIVER STEERING TORQUE (C)** receives the driver steering torque request and outputs an **activation\_status** to the **FINAL EPS TORQUE GENERATOR**.
  - FINAL EPS TORQUE GENERATOR (C)** receives the **LDW Torque Request** and the **activation\_status** from both the LDW SAFETY ACTIVATION and DRIVER STEERING TORQUE blocks. It outputs the **Final torque**.
  - CAR DISPLAY ECU** receives the **activation\_status** from the DRIVER STEERING TORQUE block.