



## 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
12/8/2018	1.0	Sindhura Buggaveeti	Initial version

### **Table of Contents**

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In <a href="Moogle Docs">Google Docs</a>, you can use headings for each section and then go to Insert > Table of Contents. <a href="Microsoft Word">Microsoft Word</a> has similar capabilities]

**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

### **Purpose**

The purpose of the software requirements and architecture document is to develop requirements and metrics against which the iteam can be verified that will ensure its functional saftey

# Inputs to the Software Requirements and Architecture Document

[Instructions:

#### **REQUIRED:**

You are only required to develop this document for the LDW (lane departure warning) amplitude malfunction. So here, provide the technical safety requirements for the LDW amplitude malfunction as well as the refined system architecture diagram from the technical safety concept.

#### **OPTIONAL:**

Expand this document to include software safety requirements for the LDW frequency malfunction as well. Go even further and document software safety requirements for the Lane Keeping Assistance (LKA) function as well.

### Technical safety requirements

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

ID	Technical Safety Requirement	A S I L	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the amplitude of the	С	50ms	LDW safety	LDW torque is set to 0

	'LDW_Torque_Request' sent to the Final electronic power steering Torque component is below 'Max_Torque_Amplitude'				
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	С	50ms	LDW safety	LDW torque is set to 0
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	С	50ms	LDW safety	LDW torque is set to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request shall be set to zero	С	50ms	Start up	LDW torque is set to 0
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in the memory	A	50ms	Data transmission integrity check	LDW torque is set to 0

### Refined Architecture Diagram from the Technical Safety Concept

[Instructions:

REQUIRED: Provide the refined system architecture diagram from the technical safety concept

# Software Requirements

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

[Instructions: Fill in the software safety requirements for the LDW amplitude malfunction technical safety requirements. We have provided the associated technical safety requirements. Hint: The software safety requirements were discussed in the text from the software and hardware lesson.

#### **OPTIONAL:**

#### CHALLENGE ONE

Develop software safety requirements for the Lane Departure Warning (LDW) frequency function and modify the system architecture as needed.

#### **CHALLENGE TWO**

Develop software safety requirements for the Lane Keeping Assistance (LKA) function and modify the system architecture as needed.

ID	Technical Safety Requirement	A S I L	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	С	50ms	LDW safety	LDW torque is set to 0

ID	Software Safety Requirement	A 0 — L	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 LA Functionality" SW component. Signal	O	LDW_SAFETY_INPUT_P ROCESSING	N/A

	"processed_LDW_Torq_Req" shall be generated at the end of the processing			
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 0 else  "limited_LDW_Torq_Req" shall take the value of  "processed_LDW_Torq_Req"	С	TORQUE_LIMITER	"limited_LDW_T orq_Req"=0(Nm =Newton-meter)
Software Safety Requirement 01-03	The limited_LDW_Torq_Req shall be transformed to "LDW_Torq_Req" which is suitable to be transmitted outside of LDW safety component to the "Final EPS Torque" component. Also see SofSafReq02-01 and SofSafReq02-02	С	LDW_SAFETY_OUTPUT _GENERATOR	LDW_Torq_Req =0(Nm=Newton- meter)

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	С	50ms	Data Transmission Integrity Check	N/A

ID	Software Safety Requirement	A S I L	7 0 0 0 0 0	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 SofSafReq03-02) shall be protected by an End2End(E2E)	С	E2ECalc	LDW_Torq_Re q=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	С	E2Ecalc	LDW_Torq_Re q=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	С	50ms	LDW Safety	LDW torque is set to 0

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_PROCESSIN G), error_status_torque_limiter(TOR QUE_LIMITER),error_status_out put_gen(LDW_SAFETY_OUTP UT_GENERATOR)	С	All	N/A
Software Safety Requirement 03-02	A software element shall evaluate the error status of all the other software elements and incase any 1 of them indicates an error, it shall deactivate the LDW feature ("activation_status"=0)	С	LDW_SAFETY _ACTIVATION	Activation_status=0(LD W function 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)	С	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_Torq_Req" is set to 0	С	All	LDW_Torq_Req=0

Software Safety Requirement 03-05	Once LDW functionality has been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again	С	LDW_SAFETY _ACTIVATION	Activation_status=0(LD W 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	С	50ms	LDW Safety	LDW torque is set to 0

ID	Software Safety Requirement	A S I L	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	С	LDW_SAFET Y_ACTIVATIO N, 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	Α	Ignition cycle	Memory Test	LDW torque is set to 0

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	MEMORYTES T	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 swicthed from off to on	Α	MEMORYTES T	Activation_status=0
Software Safety Requirement 05-03	The test result of the RAM or Flash memeory shall be indicated to the LDW_Safety component via the "test_status" signal	A	MEMORYTES T	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	Α	LDW_SAFET Y_INPUT_PR OCESSING	Activation_status=0

# Refined Architecture Diagram

