Software Safety Requirements and Architecture

Lane Assistance

Document Version: 1.1

Template Version 1.1, Released on 2018-07-02

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
7/2/18	V1.1	Aaron li	First submission

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 Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Purpose

[Instructions: Answer what is the purpose of this document?]
The purpose of this document is to define the Software Safety Requirements and Architecture for Lane Assistance.

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	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.	D	500ms	EPS ECU - Final Torque	Turn off the function completely
Technical Safety Requirement 02					
Technical Safety Requirement 03					
Technical Safety Requirement 04					
Technical Safety Requirement 05					

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**	**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	500ms	EPS ECU - Final Torque	Turn off the function completely

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 pre-processed to determine the torque request coming from the “Basic/Main LAFunctionality” SW Component. Signal “processed_LDW_Torq_Req” shall be generated at the end of the processing.	C	LDW_SAFETY_INPUT_PROCESSING	N/A
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”.	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 SofSafReq02-01 and SofSafReq02-02	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 02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	500ms	EPS ECU - Final Torque	Turn off the function completely

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 02-01	Signal should be validated	C	LDW_SAFETY_INPUT_PROCESSING	Limited output
Software Safety Requirement 02-02	Signal should be verified	C	LDW_SAFETY_OUTPUT_GENERATOR	Limited output

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	500ms	EPS ECU - Final Torque	Turn off the function completely

ID	Software Safety Requirement	A S I L	Allocation Software Elements	Safe State
Software Safety Requirement 03-01	Signal should be validated	C	LDW_SAFETY_INPUT_PROCESSING	Limited output
Software Safety Requirement 03-02				
Software Safety Requirement 03-03				
Software Safety Requirement 03-04				
Software Safety Requirement 03-05				

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	500ms	EPS ECU - Final Torque	Turn off the function completely

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 04-01	Signal should be validated	C	LDW_SAFETY_INPUT_PROCESSING	Limited output

ID	Technical Safety Requirement	ASIL	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	C	500ms	EPS ECU - Final Torque	Turn off the function completely

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 05-01	Signal should be validated	C	EPS ECU	idled
Software Safety Requirement 05-02				
Software Safety Requirement 05-03				
Software Safety Requirement 05-04				

Refined Architecture Diagram

[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the software and hardware lesson, including all of the ASIL labels.]