Elektrobit

UDACITY

Software Safety Requirements and Architecture

Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
June 21, 2017	1.0	Udacity, EB	Template version
April 26, 2019	1.1	Ahmed Belal	Finalize the document

Table of Contents

Purpose

The purpose of this document is to get into more details of the technical safety concept (TSC) by deriving software safety requirements from technical safety requirements. Software requirements are much more specific than technical requirements. Software requirements specify variable names, signal paths, and software protocols and mechanisms. A software engineer should be able to write a program from the software requirements and software architecture.

Inputs to the Software Requirements and Architecture Document

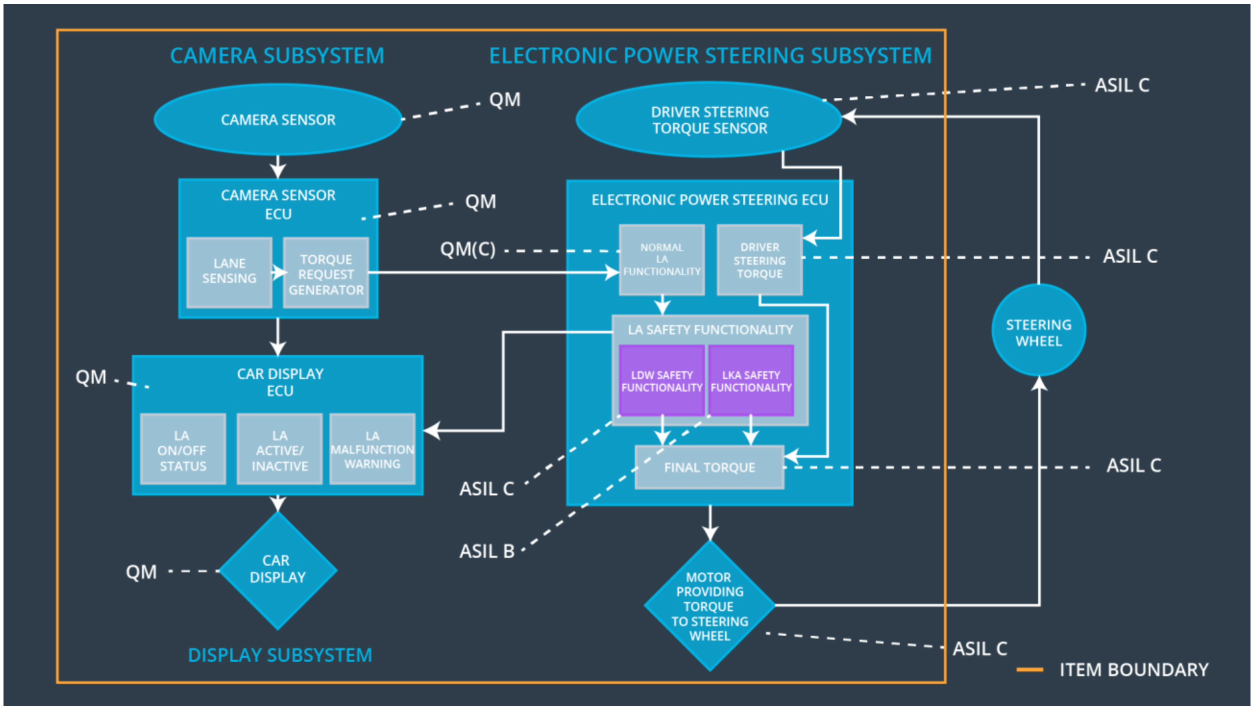
Technical safety requirements

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 lane departure warning (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	50ms	LDW Safety block	Shut down the LDW system by setting 'LDW_Torque_Request' to zero
Technical Safety Requirement 02	The validity and integrity of data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50ms	Data Transmission Integrity Check	Shut down the LDW system by setting 'LDW_Torque_Request' to zero
Technical Safety Requirement 03	As soon as failure detected by lane departure warning (LDW) function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall set to zero	C	50ms	LDW Safety block	Shut down the LDW system by setting 'LDW_Torque_Request' to zero

Technical Safety Requirement 04	As soon as the LDW function deactivate the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light	C	50ms	LDW Safety block	Shut down the LDW system by setting 'LDW_Torque_Request' to zero
Technical Safety Requirement 05	Memory tests shall be conducted at startup of the EPS ECU to check for any faults in memory	A	Length of the vehicle ignition cycle	Memory Tests Check	Restart the LDW system, if this repeated for 3 times, display error signal on the car display

Refined Architecture Diagram from the Technical Safety Concept



Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

Technical Safety Requirement 01

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The lane departure warning (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	50ms	LDW Safety block	Shut down the LDW system by setting 'LDW_Torque_Request' to zero

Software Safety requirements for Technical Safety Requirement 01

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, and 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)

Technical Safety Requirement 02

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02	The validity and integrity of data transmission for ‘LDW_Torque_Request’ signal shall be ensured	C	50ms	Data Transmission Integrity Check	Shut down the LDW system by setting ‘LDW_Torque_Request’ to zero

Software Safety requirements for Technical Safety Requirement 02

ID	Software Safety Requirement	ASIL	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 SofSafReq03-02) 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)

Technical Safety Requirement 03

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 03	As soon as failure detected by lane departure warning (LDW) function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall set to zero	C	50ms	LDW Safety block	Shut down the LDW system by setting 'LDW_Torque_Request' to zero

Software Safety requirements for Technical Safety Requirement 03

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement03-01	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 Requirement03-02	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 Requirement03-03	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 Requirement03-04	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	C	All	LDW_Torq_Req = 0
Software Safety Requirement03-05	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_ACTIVATION	Activation_status = 0 (LDW function deactivated)

Technical Safety Requirement 04

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 04	As soon as the LDW function deactivate the LDW feature, the ‘LDW Safety’ software block shall send a signal to the car display ECU to turn on a warning light	C	50ms	LDW Safety block	Shut down the LDW system by setting ‘LDW_Torque_Request’ to zero

Software Safety requirements for Technical Safety Requirement 04

ID	Software Safety Requirement	ASIL	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 displayECU.	C	LDW_SAFETY_ACTIVATION, CarDisplay ECU	N/A

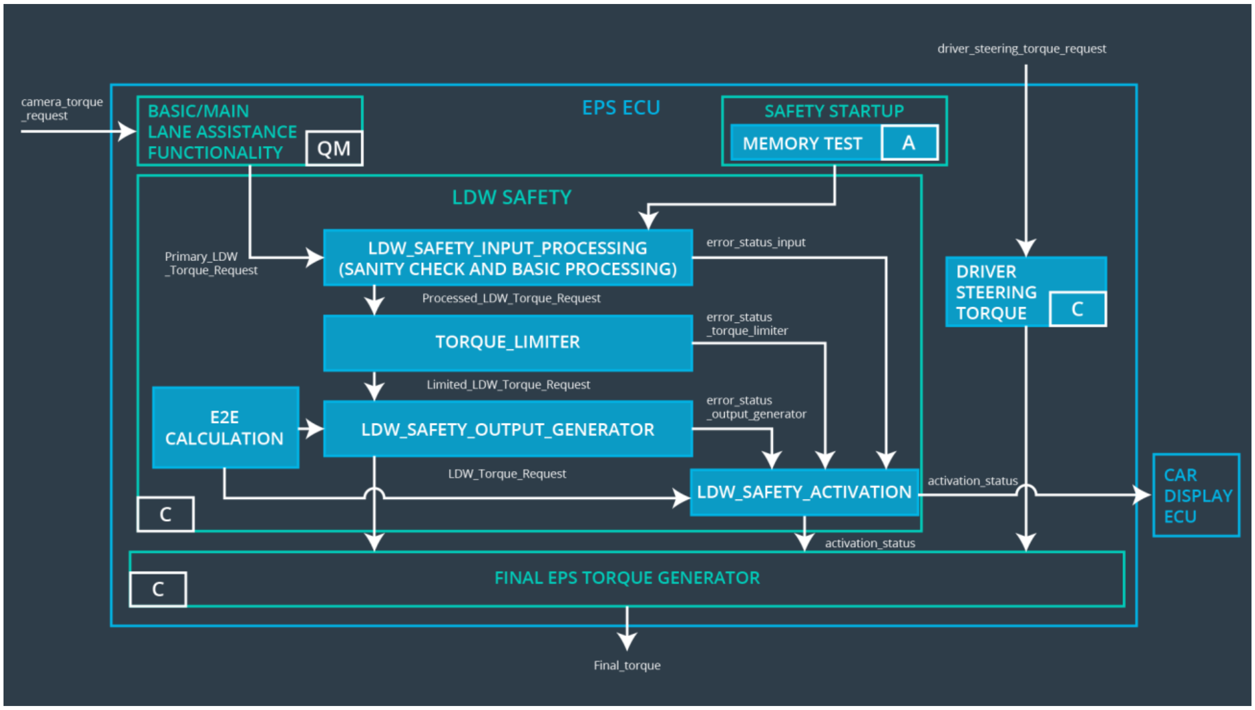
Technical Safety Requirement 05

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	Memory tests shall be conducted at startup of the EPS ECU to check for any faults in memory	A	Length of the vehicle ignition cycle	Memory Tests Check	Restart the LDW system, if this repeated for 3 times, display error signal on the car display

Software Safety requirements for Technical Safety Requirement 05

ID	Software Safety Requirement	ASIL	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

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
C
DRIVER STEERING TORQUE
C
activation_status
CAR DISPLAY ECU
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque