Elektrobit

UDACITY

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
2018-03-26	1.0	Felipe A. L. Reis	First submission.

Table of Contents

Purpose

The main purpose of this document is define the software safety requirements and architecture. This documents will use Technical Safety Requirements to provide detailed software requirements, with metrics that can be measured and ensure the software quality in order to achieve the reduction of risks into a acceptable level.

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 Req. 01	“The LDW component shall ensure the amplitude of ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering torque’ component is below ‘Max_Torque_Amplitude” [1]	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.
Technical Safety Req. 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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.
Technical Safety Req. 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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.
Technical Safety Req. 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall	C	50ms	Data Transmission Integrity	Set the vibration torque to

	be ensured.				zero.
Technical Safety Req. 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Check Integrity	Set the vibration torque to zero.

Table 1. Technical Safety Requirements

Refined Architecture Diagram from the Technical Safety Concept

The refinement of the Lane Assistance System Architecture is shown in Image 1. The refined system architecture contains some tests to identify integrity of the data, safety tests and other resources to prevent failures. Also, this architecture contains some information about the risks ASIL, derived from each part of the system.

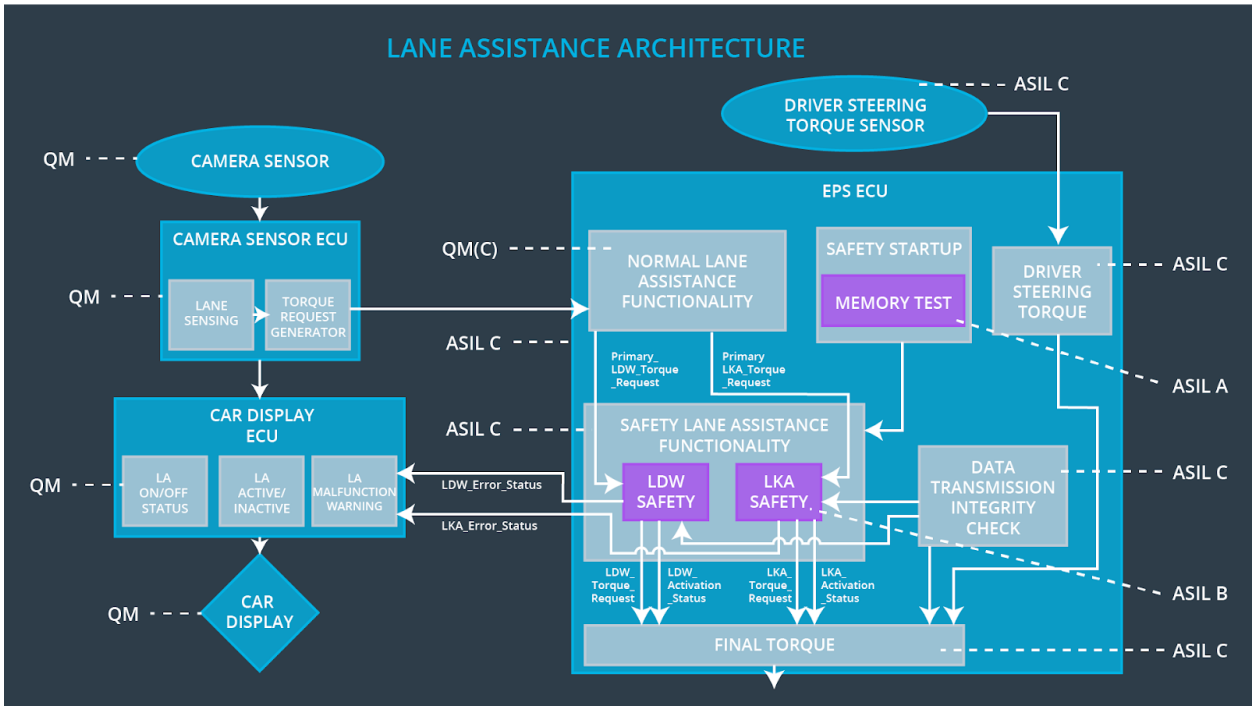

Image 1. Refined Lane Assistance System Architecture

Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Req. 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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.

Table 2. Functional Safety Requirements - Lane Departure Warning

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Req. 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 ‘processed_LDW_Torq_Req’ shall be generated at the end of the processing”. [2]	C	LDW_SAFETY_INPUT_PROCESSING	N/A
Software Safety Req. 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’”. [2]	C	TORQUE_LIMITER	“limited_LDW_Torq_Req” = 0 (Nm=Newton-meter)
Software Safety Req. 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	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

	the ‘Final EPS Torque’ component. Also see SSR02-01 and SSR02-02”. [2]			

Table 3. Software Safety Requirements - Lane Departure Warning

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Req. 02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.

Table 4. Functional Safety Requirements - Lane Departure Warning

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Req. 02-01	“Any data to be transmitted outside of the LDW Safety component (‘LDW Safety’) including ‘LDW_Torque_Req’ and ‘activation_status’ (see SSR 03-02) shall be protected by an End2End(E2E) protection mechanism”. [2]	C	E2ECalc	LDW_Torq_Req = 0 (Nm)
Software Safety Req. 02-02	“The E2E protection protocol shall contain and attach the control data: alive counter (SQC) and CRC to the data to be transmitted”. [2]	C	E2ECalc	LDW_Torq_Req = 0 (Nm)

Table 5. Software Safety Requirements - Lane Departure Warning

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Req. 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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	Set the vibration torque to zero.

Table 6. Functional Safety Requirements - Lane Departure Warning

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Req. 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_PROCESSING), error_status_torque_limiter(TORQUE_LIMITER), error_status_output_gen(LDW_SAFETY_OUTPUT_GENERATOR) C”. [2]	C	All	N/A
Software Safety Req. 03-02	“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)”. [2]	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)
Software Safety Req. 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)”	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Req. 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”. [2]	C	All	LDW_Torq_Req = 0
Software Safety Req. 03-05	“Once the LDW functionality has been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again”. [2]	C	LDW_SAFETY_ACTIVATION	Activation_status = 0 (LDW function deactivated)

Table 7. Software Safety Requirements - Lane Departure Warning

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Req.	As soon as the LDW function deactivates the LDW feature, the			EPS ECU - Lane Departure	Set the vibration

04	LDW Safety software block shall send a signal to the car display ECU to turn on a warning light	C	50ms	Warning Safety Functionality	torque to zero.

Table 8. Functional Safety Requirements - Lane Departure Warning

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Req. 04-01	“When the LDW function is deactivated (activation_status set to 0), the activation_status shall be sent to the car display ECU”. [2]	C	LDW_SAFETY_ACTIVATION, CarDisplay ECU	N/A

Table 9. Software Safety Requirements - Lane Departure Warning

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Req. 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition cycle	Memory Check Integrity	Set the vibration torque to zero.

Table 10. Functional Safety Requirements - Lane Departure Warning

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Req. 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”. [2]	A	MEMORYTEST	Activation_status = 0
Software Safety Req. 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)”. [2]	A	MEMORYTEST	Activation_status = 0

Software Safety Req. 05-03	“The test result of the RAM or Flash memory shall be indicated to the LDW_Safety component via the ‘test_status’ signal”. [2]	A	MEMORYTEST	Activation_status = 0
Software Safety Req. 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 LDW Torque is set to 0”. [2]	A	LDW_SAFETY_INPUT_PROCESSING	Activation_status = 0

Table 11. Software Safety Requirements - Lane Departure Warning

Refined Architecture Diagram

The refinement of the Lane Assistance System Architecture is shown in Image 2 and 3. Image 2 contains a architecture the whole system architecture and how components interacts with each other. Also contains ASIL risks for each part of the system.

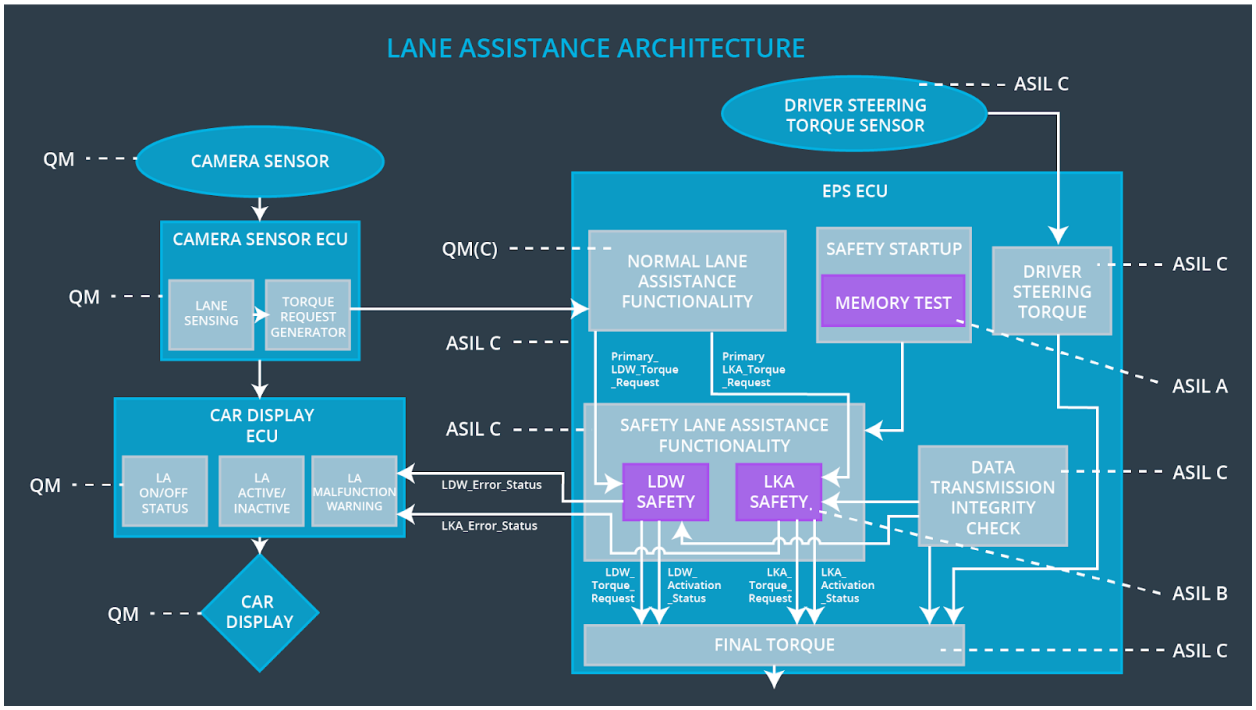

Image 2. Refined Lane Assistance System Architecture

Image 3 shows the EPS ECU component in a much more detailed level than Image 2. Image 3 contains the LDW safety information, ASIL risks and how the small components interacts with each other with technical and software information.

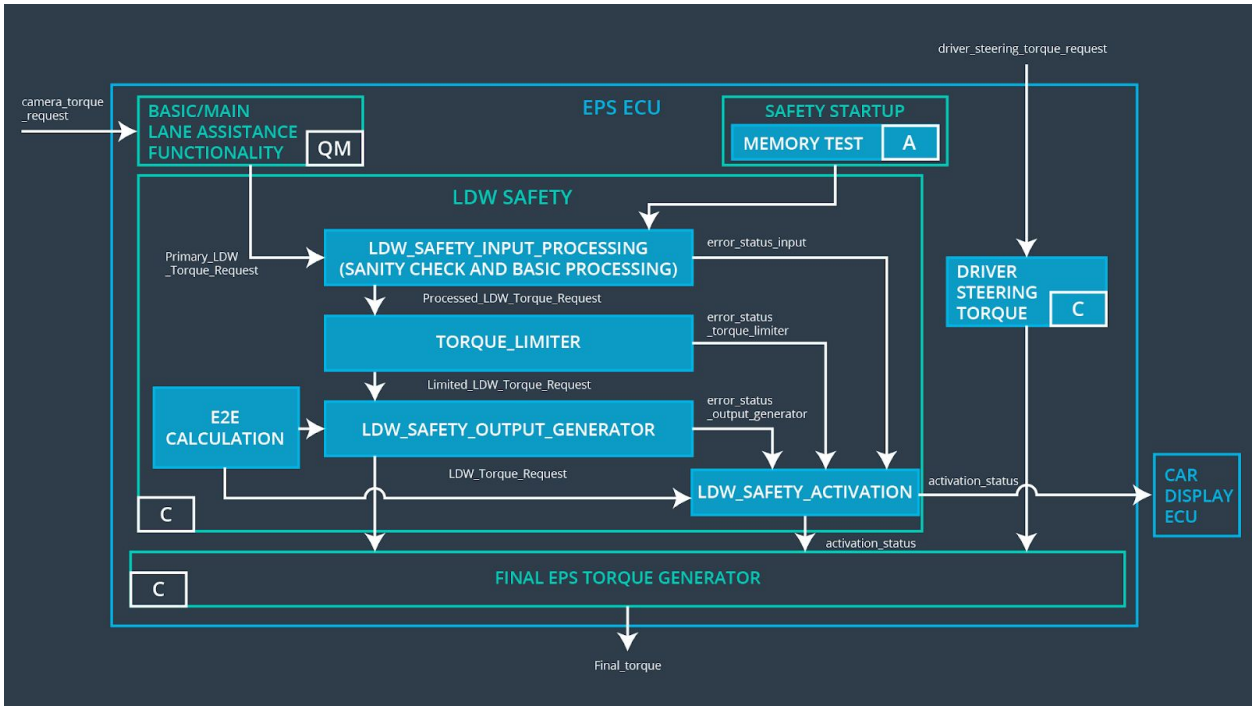

Image 3. EPS ECU Architecture

References

[1] Functional Safety: Deriving Technical Safety Requirements. **Udacity**. Available in: https://classroom.udacity.com/nanodegrees/nd013/parts/6047fe34-d93c-4f50-8336-b70ef10cb4b2/modules/6dc3d743-2b0f-4ae6-97b7-e2ff866f17ef/lessons/9734ccc4-75e5-4f7f-9f1f-483355714308/concepts/789309bf-c4f0-4a17-ae81-cc26d0fc6709. Accessed in 2018-03-27.

[2] Functional Safety at Software and Hardware Levels: Software Safety Requirements Lane Departure Warning. **Udacity**. Available in: https://classroom.udacity.com/nanodegrees/nd013/parts/6047fe34-d93c-4f50-8336-b70ef10cb4b2/modules/6dc3d743-2b0f-4ae6-97b7-e2ff866f17ef/lessons/6c774579-9d59-43fe-8e0e-0700dd440861/concepts/8c465c10-b05a-4b62-aec7-18e2b2f16141. Accessed in 2018-03-28.