Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 2.0

Version 1.0, Released on 2018-04-28

Document history

Date	Version	Editor	Description
04/28/2018	1.0	Ninad Ghike	Initial Creation
05/15/2018	2.0	Ninad Ghike	Update safe state

Table of Contents

Purpose of the Technical Safety Concept

Technical Safety Concept (TSC) is part of the product development phase. Though it looks similar to Functional Safety Concept but it is more concrete and goes into the technical details of the item's technology. TSC often define the signal flow and covers the general hardware and software requirements without going into the specific details.

Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 msec	LDW will set the oscillating torque amplitude to 0
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 msec	LDW will set the oscillating torque amplitude to 0
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 msec	LDW will set the oscillating torque amplitude to 0

Refined System Architecture from Functional Safety Concept

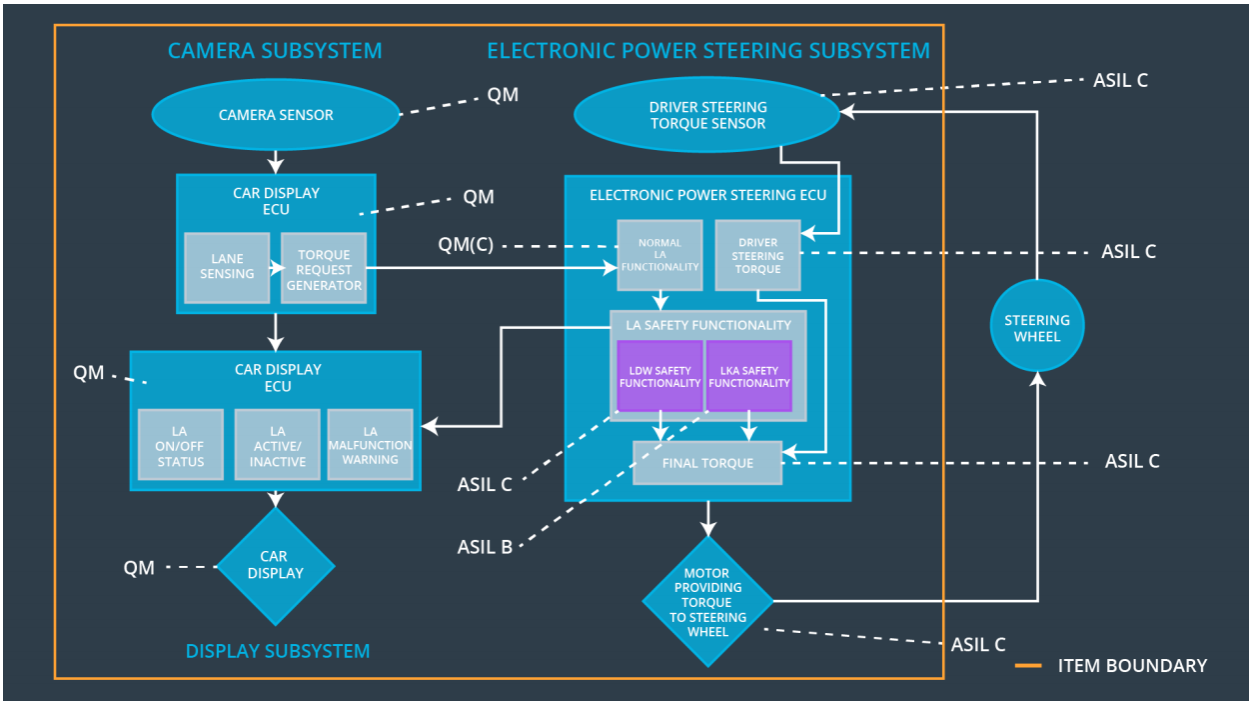


Figure 1

Functional overview of architecture elements

Element	Description
Camera Sensor	The Camera Sensor reads in images from the road
Camera Sensor ECU - Lane Sensing	The Camera Sensor ECU - Lane Sensing defines lane departure
Camera Sensor ECU - Torque request generator	The Camera Sensor ECU - Torque request generator sends torque request to EPS ECU
Car Display	Takes the input from car display ECU and displays on/off warning sign as well as any malfunction occurred.
Car Display ECU - Lane Assistance On/Off Status	Shows light on and off for LA symbol if driver turn LAS on and off.
Car Display ECU - Lane Assistant Active/Inactive	Shows light on and off for LA symbol if LDW or LKS activated or deactivated.
Car Display ECU - Lane Assistance malfunction warning	The Car Display ECU - LA malfunction warning controls a warning light that tells the driver if the LA has a malfunction
Driver Steering Torque Sensor	The Driver Steering Torque Sensor measures steering torque provided by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The EPS ECU - Driver Steering Torque receives a signal from Driver Steering Torque Sensor, processes and sends steering torque provided by the driver to EPS ECU - Final Torque
EPS ECU - Normal Lane Assistance Functionality	The EPS ECU - Normal LA Functionality processes and sends request satisfying normal functionality
EPS ECU - Lane Departure Warning Safety Functionality	The EPS ECU - LDW Safety Functionality processes and checks that vibrational request not above limits
EPS ECU - Lane Keeping Assistant Safety Functionality	The EPS ECU - EPS ECU - LKA Safety Functionality processes and checks that torque request not above limits
EPS ECU - Final Torque	Sends the final required torque value to the motor.
Motor	Takes the input from EPS ECU and applies the torque to the steering wheel.

Technical Safety Concept

Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:
Functional Safety Requirement 01-01 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	X		

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 msec	LDW Safety Functionality	LDW will set the oscillating torque amplitude to 0
Technical Safety Requirement 02	The 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light as soon as the LDW function deactivates the LDW feature.	C	50 msec	LDW Safety Functionality	LDW will set the oscillating torque amplitude to 0
Technical Safety Requirement 03	The LDW function shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero as soon as a failure is detected.	C	50 msec	LDW Safety Functionality	LDW will set the oscillating torque amplitude to 0

Technical Safety Requirement 04	The system shall check for the timeouts of 'LDW_Torque_Request' Signal	C	50 msec	Data Transmission integrity check	LDW will set the oscillating torque amplitude to 0
Technical Safety Requirement 05	The system shall perform memory check of the EPS ECU at bootup to look for memory related faults.	A	Ignition Cycle	Safety Startup	LDW will set the oscillating torque amplitude to 0

Functional Safety Requirement 01-02 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01-02-01	The LDW safety component shall ensure that the frequency of the "LDW_Torque_Request" sent to the "EPS ECU - Final Torque" component is below Max_Torque_Frequency	C	50 ms	LDW Safety block	LDW torque request shall be set to zero
Technical Safety Requirement	As soon as the LDW function deactivates the LDW feature, the "LDW Safety" software block shall	C	50 ms	LDW Safety block	LDW torque request

01-02-02	send a signal to the car display ECU to turn on a warning light				shall be set to zero
Technical Safety Requirement 01-02-03	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 block	LDW torque request shall be set to zero
Technical Safety Requirement 01-02-04	The validity and integrity of the data transmission for “LDW_Torque_Request” signal shall be ensured	C	50 ms	Data Transmission Integrity Check block	LDW torque request shall be set to zero
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	ignition cycle	Safety Startup Memory Test block	LDW torque request shall be set to zero

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

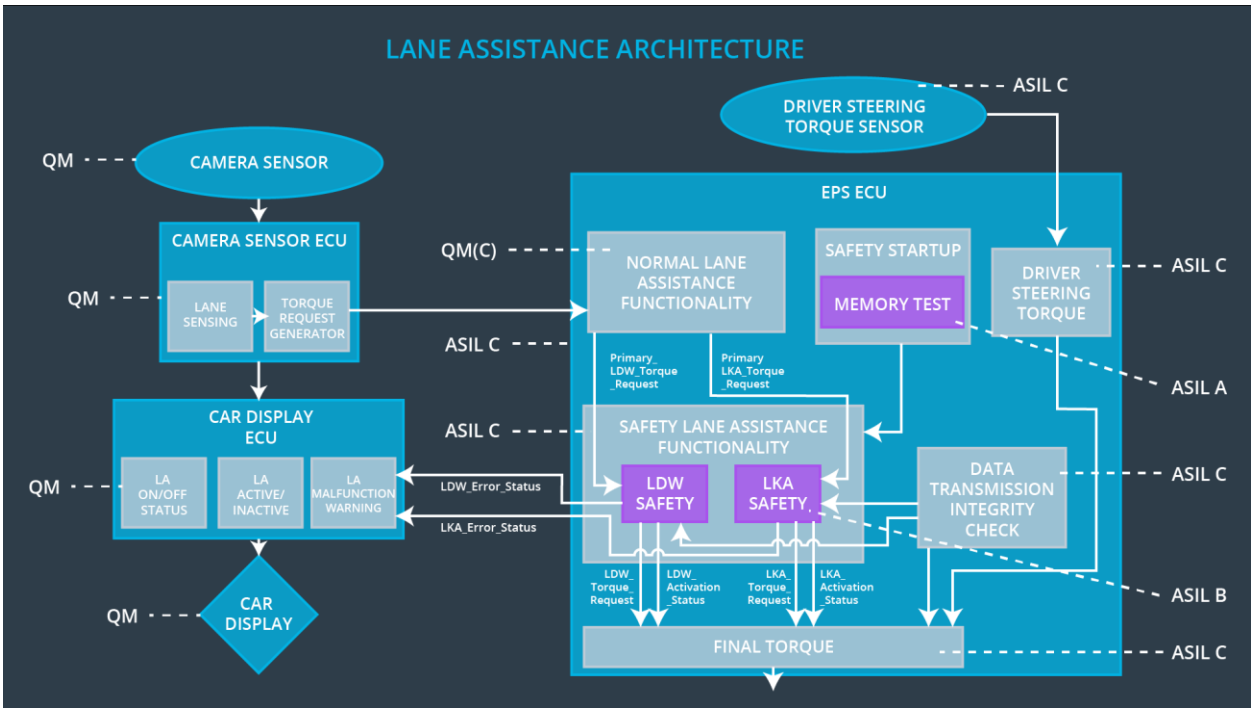
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure that the torque request of the “LKA_Torque_Request” sent to the 'EPS ECU - Final Torque' component is applied for only Max_Duration	B	500 ms	LKA Safety block	LKA torque request shall be set to zero
Technical Safety Requirement 02-01-02	As soon as the LKA function deactivates the LKA feature, the “LKA Safety” software block shall send a signal to the car display ECU to turn on a warning light	B	500 ms	LKA Safety block	LKA torque request shall be set to zero
Technical Safety Requirement 02-01-03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the “LKA_Torque_Request” shall be set to zero	B	500 ms	LKA Safety block	LKA torque request shall be set to zero
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for “LKA_Torque_Request” signal shall be ensured	B	500 ms	Data Transmission Integrity Check block	LKA torque request shall be set to zero
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	ignition cycle	Safety Startup Memory Test block	LKA torque request shall be set to zero

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For Lane Assistance system, which includes LDW and LKA, all technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Vibrational torque request received by the Electronic Power Steering ECU is very high	Vibrational torque request is higher than MAX_Torque_Amplitude or MAX_Torque_Frequency	Yes	Display a malfunction warning light on the driver dashboard
WDC-02	Duration of the LKA torque request received by the electronic power steering ECU is long	Duration of torque request is more than Max_Duration	Yes	Display a malfunction warning light on the driver dashboard