Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0
Released on 2017-10-29

Document history

Date	Version	Editor	Description
10/29/2017	1.0	Trevor Conley	First Submission

Table of Contents

Purpose of the Technical Safety Concept

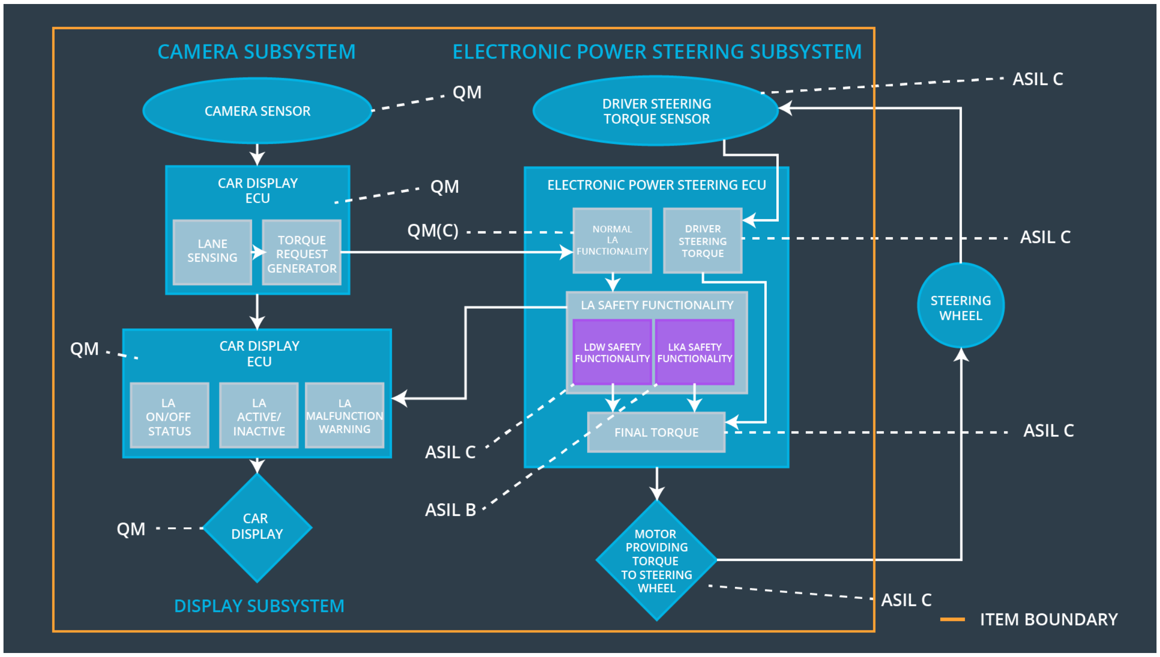
The Technical Safety Conccept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

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 requested by the LDW is below MAX_TORQUE_AMPLITUDE	C	50 ms	LDW will set oscillating torque amplitude to 0
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below MAX_TORQUE_FREQUENCY	C	50 ms	LDW will set oscillating torque amplitude to 0
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the lane keeping assistance torque is only applied for MAX_DURATION	B	500 ms	Set lane keeping assistance torque to 0
Functional Safety Requirement 02-02	The Electronic Power Steering ECU shall ensure that the lane keeping assistance torque is set to 0 when the Camera Sensor ECU stops detecting lane markings and shall send an ‘off’ status to the Car Display	B	500 ms	Set lane keeping assistance torque to 0

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Sensor responsible for capturing vehicle diving condition including lane markings
Camera Sensor ECU - Lane Sensing	Software Module in the Camera Subsystem reponsible for detecting lane lines and determining when the vehicle mistakenly departs the lane
Camera Sensor ECU – Torque reqest generator	Software Module in the Camera Subsystem responsible for calculating and sending additional torque to the LDW and LKA functions
Car Display	Visual display responsible for displaying warning of lane departure and LDW and LKA activations/deactivations
Car Display ECU – Lane Assistance On/Off Status	Visual display responsible for displaying LDW and LKA status
Car Display ECU – Lane Assistance Active/Inactive	Visual display responsible for displaying the warning of lane departure, LDW and LKA activations/deactivations
Car Display ECU – Lane	Visual display responsible for displaying warning of LDW and

Assistance malfunction warning	LKA malfunctions
Driver Steering Torque Sensor	Sensor responsible for measuring how much steering torque the driver is applying to the steering wheel
Electronic Power Steering (EPS) ECU – Driver Steering Torque	Software Module in the Electronic Power Steering ECU responsible for receiving the Camera Sensor ECU torque resquest
EPS ECU – Normal Assistance Functionality	Software Module in the Electronic Power Steering ECU responsible for receving the Driver Steering Torque Sensor input from the steering wheel
EPS ECU – Lane Departure Warning Safety Functionality	Software Module in the Electronic Power Steering ECU responsible for keeping the lane departure oscillating torque and frequency below the MAX_TORQUE_AMPLITUDE and MAX_TORQUE_FREQUENCY
EPS ECU – Lane Keeping Assistant Safety Functionality	Software Module in the Electronic Power Steering ECU responsible for ensuring the time of the lane departure oscillating torque freqeuncy and amplitude does not exceed MAX_DURATION, and if the lane is lost the LKA function is deactivated
EPS ECU – Final Torque	Software Module in the Electronic Power Steering ECU responsible for ensuring the LDW, LKA, and driver’s steering torque requests are combined and sent to the motor
Motor	Provides torque to the steering wheel

Technical Safety Concept

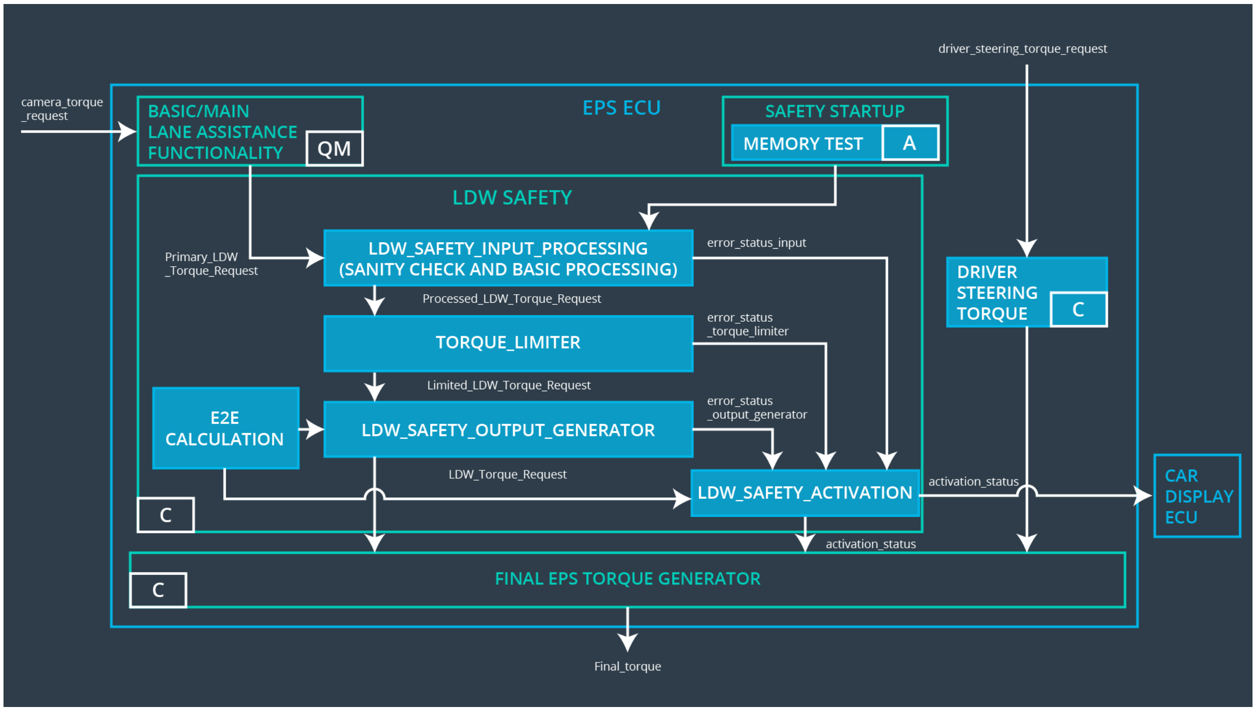
Technical Safety Requirements

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:

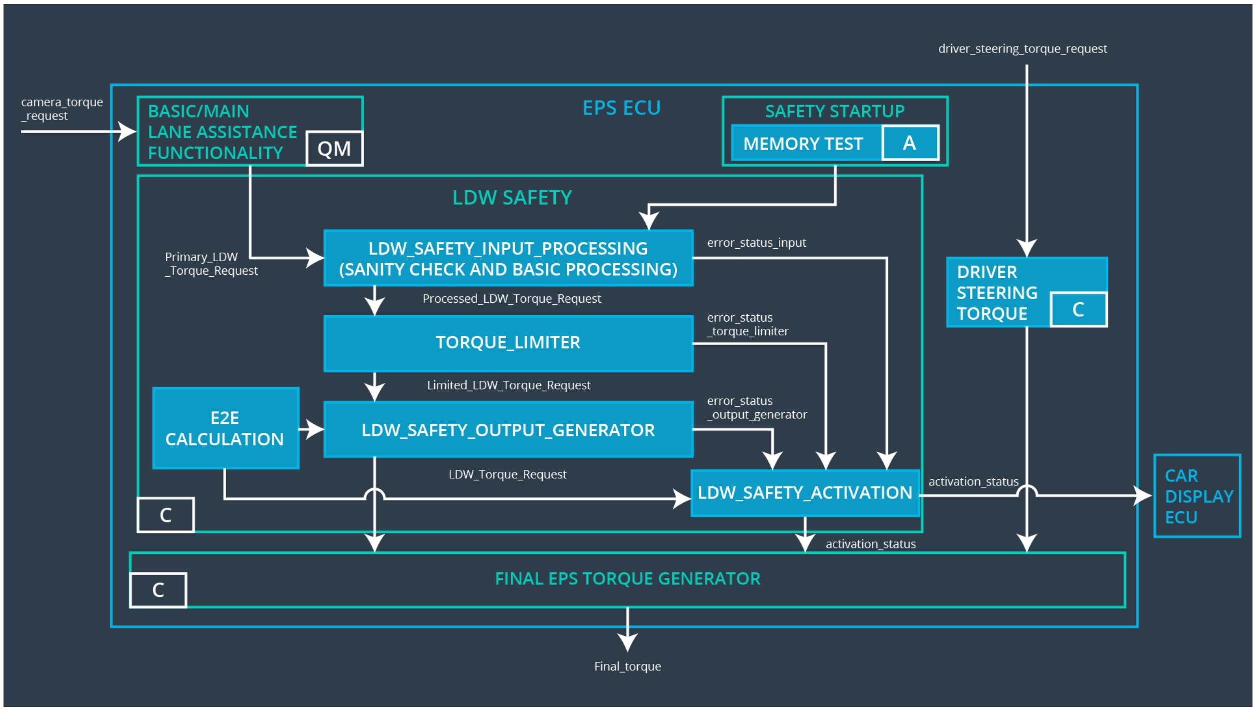

driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
C
activation_status
DRIVER STEERING TORQUE
C
CAR DISPLAY ECU
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

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 ms	LDW Safety Block	The lane departure warning torque is set to 0
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.	C	50 ms	LDW Safety Block	The lane departure warning 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.	C	50 ms	LDW Safety Block	The lane departure warning torque is set to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	LDW Safety Block	The lane departure warning 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 memory.	A	Ignition cycle	Safety Startup	The lane departure warning torque is set 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:


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
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
activation_status
CAR DISPLAY ECU
C
activation_status
FINAL EPS TORQUE GENERATOR
C
Final_torque

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 ‘Final electronic power steering Torque’ component is below MAX_TORQUE_FREQUENCY	C	50 ms	LDW Safety Block	The lane departure warning torque is set to 0

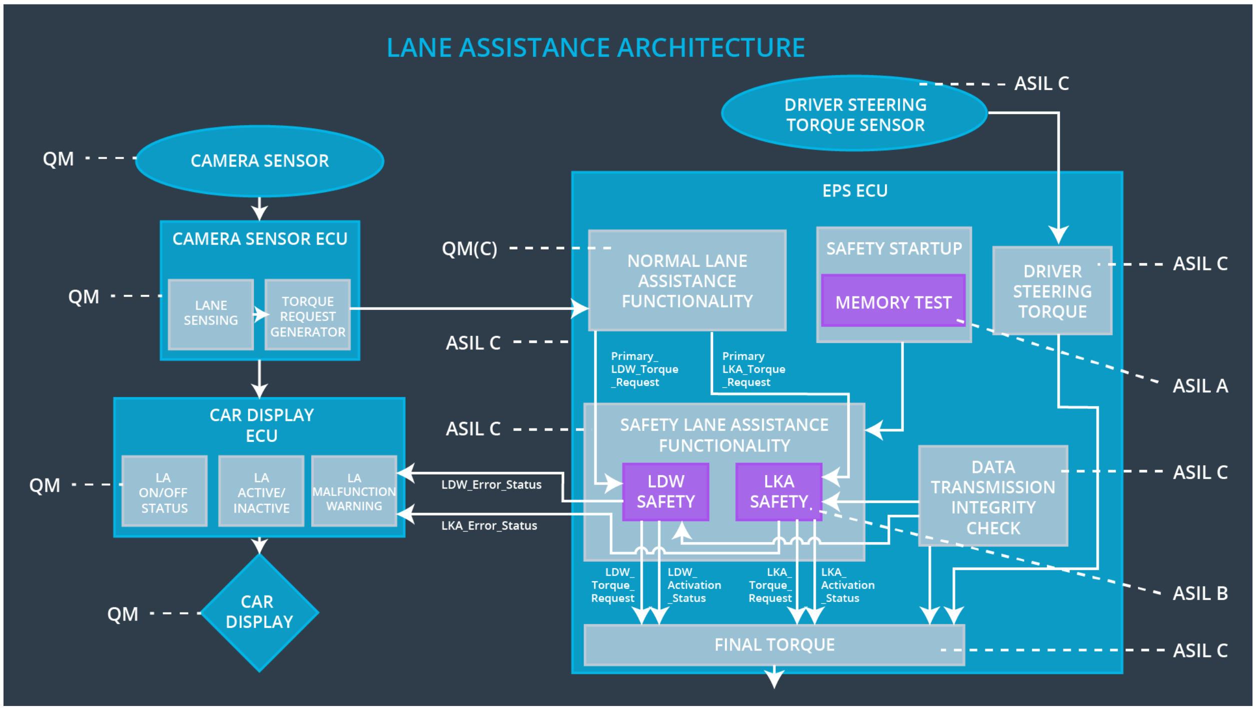
Lane Keeping Assistance (LKA) Requirements:
Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

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 01	The LKA safety component shall ensure that the duration of the lane keeping assistance torque is applied no longer than MAX_DURATION	C	500 ms	LKA Safety Block	The lane keeping assistance torque is set to 0
Technical Safety Requirement 02	As soon as the LKA function deactivates its feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light	C	500 ms	LKA Safety Block	The lane keeping assistance torque is set to 0
Technical Safety Requirement 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 0	C	500 ms	LKA Safety Block	The lane keeping assistance torque is set to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for the 'LKA_Torque_Request' signal shall be ensured	C	500 ms	LKA Safety Block	The lane keeping assistance torque is set to 0
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any memory faults	A	Ignition start	Safety Startup	The lane keeping assistance torque is set to 0

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements in this tiem 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	Turn of LDW funcionality	Malfunction_01, Malfunction_02	Yes, LDW torque shall be 0	Lane Assistance inactive and Malfunction Warning will be set in the Car Display ECU
WDC-02	Turn off LKA functionality	Malfunction_03, Malfunction_04	Yes, LKA torque shall be 0	Lane Assistance inactive and Malfunction Warning will be set in the Car Display ECU