Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 2.0

Document history

Date	Version	Editor	Description
08/08/2017	1.0	Thomas Ho	Initial Release
08/11/2017	2.0	Thomas Ho	Revised based on review feedback

Table of Contents

Purpose of the Technical Safety Concept

The purpose of this document is to specify technical safety requirement based on functional safety requirements, and allocate technical safety requirements to the system architecture.

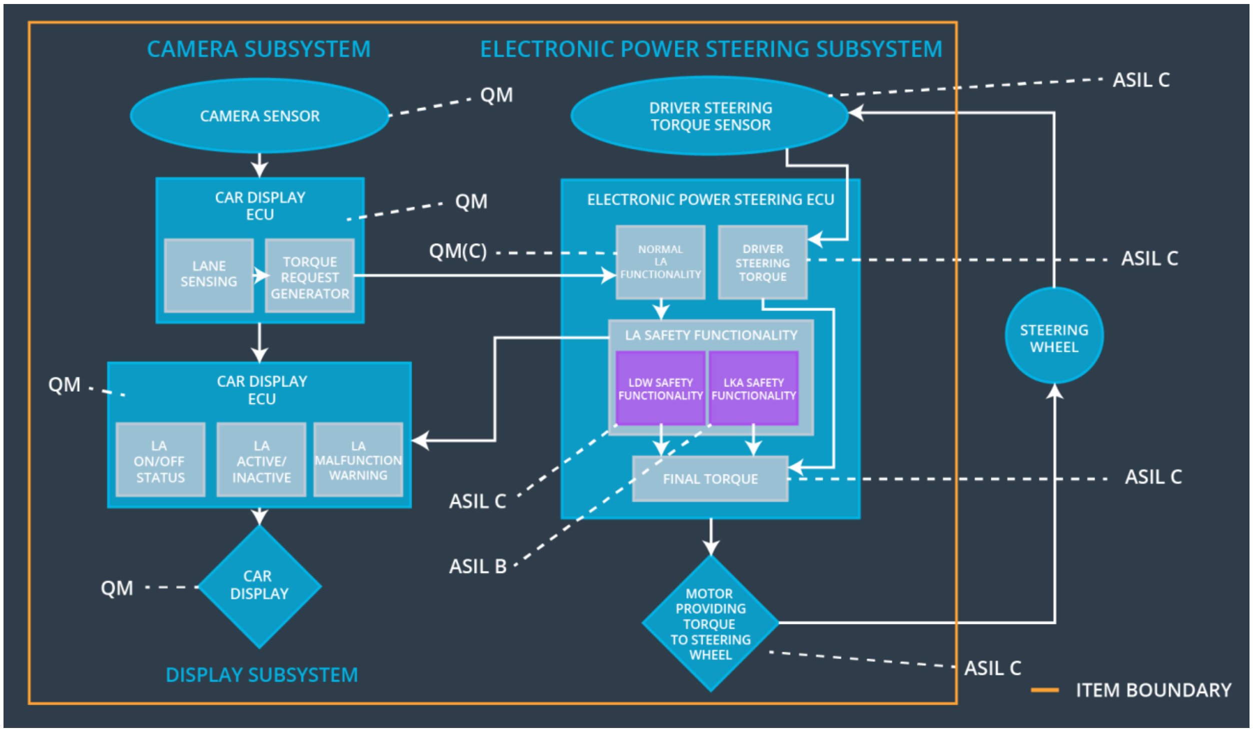
Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The electronic power steering subsystem shall ensure that the oscillating torque amplitude is less than Max_Torque_Amplitude	C	50 ms	OFF
Functional Safety Requirement 01-02	The electronic power steering subsystem shall ensure that the oscillating torque frequency is less than Max_Torque_Frequency	C	50 ms	OFF
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	OFF

Refined System Architecture from Functional Safety Concept

The refined system architecture is shown on following figure.



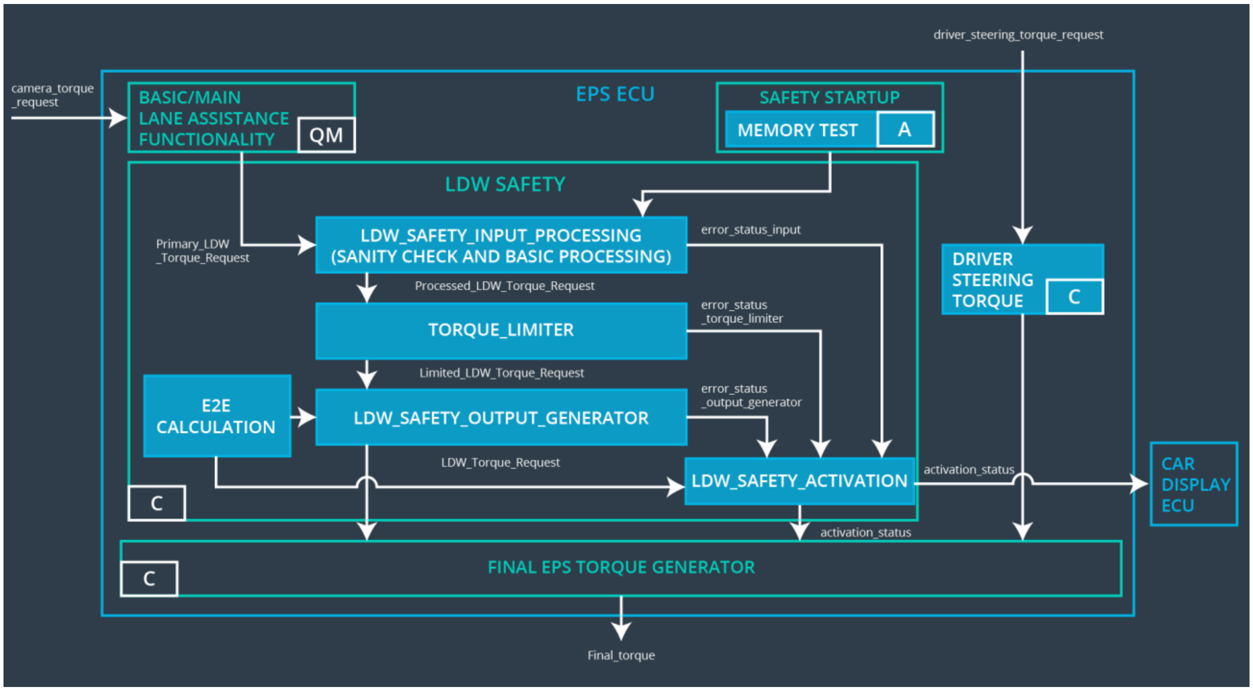
Functional overview of architecture elements

Element	Description
Camera Sensor	Capture and stream images to Camera Sensor ECU for processing
Camera Sensor ECU - Lane Sensing	Detect the lane and check if the vehicle is moving away from the ego lane
Camera Sensor ECU - Torque request generator	Responsible for sending a torque request to the electronic power steering subsystem
Car Display	Graphic interface used to display the warning messages and setting changes etc.
Car Display ECU - Lane Assistance On/Off	Controlling a light that tells the driver if the lane

Status	keeping system on or off.
Car Display ECU - Lane Assistant Active/Inactive	Controlling a light telling the driver that if the lane departure warning is activated.
Car Display ECU - Lane Assistance malfunction warning	Displaying warning message if LA system is malfunctioning
Driver Steering Torque Sensor	Responsible for measuring the torque applied by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Sends the information to the EPS ECU Final Torque about the torque applied by the driver sensed by the Driver Steering Torque sensor.
EPS ECU - Normal Lane Assistance Functionality	Sends Vibrational_Torque_Request to the Lane Departure Warning Safety Software element.
EPS ECU - Lane Departure Warning Safety Functionality	Alert driver when vehicle start deviating from its lane by applying oscillating torque to steering wheel. The oscillating torque amplitude is limited to be less than Max_Torque_Amplitude, the frequency is less than Max_Torque_Frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	Applying an amount of torque no longer than Max_Duration to help the car to stay in the lane.
EPS ECU - Final Torque	Add torque requests together to output a final torque to the motor that move the steering wheel.
Motor	Actuator used to apply requested torque to steering wheel.

Technical Safety Concept

Technical Safety Requirements


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
C
FINAL EPS TORQUE GENERATOR
Final_torque

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 ms	LDW Safety block	Off
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	Off
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	Off
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Checking	Off
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	Memory Test	Off

Functional Safety Requirement 01-2 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	A S IL	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_Frequency.	C	50 ms	LDW Safety block	Off
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	Off
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	Off

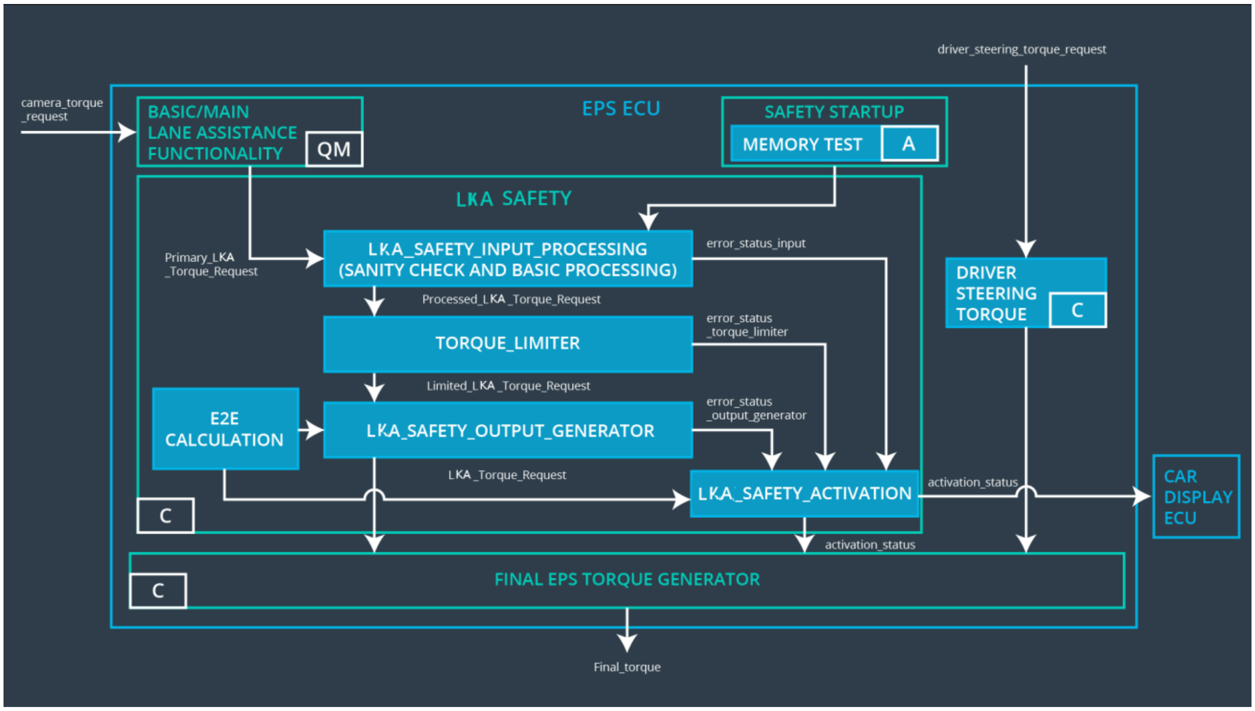
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.		50 ms	Data Transmission Integrity Checking	Off
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Memory Test	Off

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria	Verification Acceptance Criteria
Technical Safety Requirement 01-01-01	Validate that the Max_Torque_Amplitude is chosen from LDW validation acceptance criteria	Verify that the amplitude of the ‘LDW_Torque_Request’ sent is always below ‘Max_Toque_Amplitude’
Technical Safety Requirement 01-01-02	Validate that error_status_xxx message is sent to LDW_SAFETY_ACTIVATION when errors occur	Verify the LDW function is deactivated when error status received, and display ECU turns on warning light
Technical Safety Requirement 01-01-03	Validate a zero LDW_Torque_Request is sent to LDW_SAFETY_ACTIVATION as soon as a failure is detected by LDW	Verify the LDW_SAFETY_ACTIVATION receives a zero LDW_Torque_Request when a failure is detected
Technical Safety Requirement 01-01-04	Validate appropriate algorithms are chosen for checking validity and integrity of the data transmission	Verify the validity and integrity of data transmission for ‘LDW_Torque_Request’ signal is implemented
Technical Safety Requirement 01-01-05	Validate the algorithm used to test memory can detect any fault in memory	Verify memory test is conducted at start up of the EPS ECU
Technical	Validate that the	Verify that the frequency of the

Safety Requirement 01-02-01	Max_Torque_Frequency is chosen from LDW validation acceptance criteria	‘LDW_Torque_Request’ sent is always below ‘Max_Toque_Frequency’

Lane Keeping Assistance (LKA) Requirements:


driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LKA SAFETY
Primary_LKA_Torque_Request
LKA_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LKA_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LKA_Torque_Request
E2E CALCULATION
LKA_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LKA_Torque_Request
LKA_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque

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:

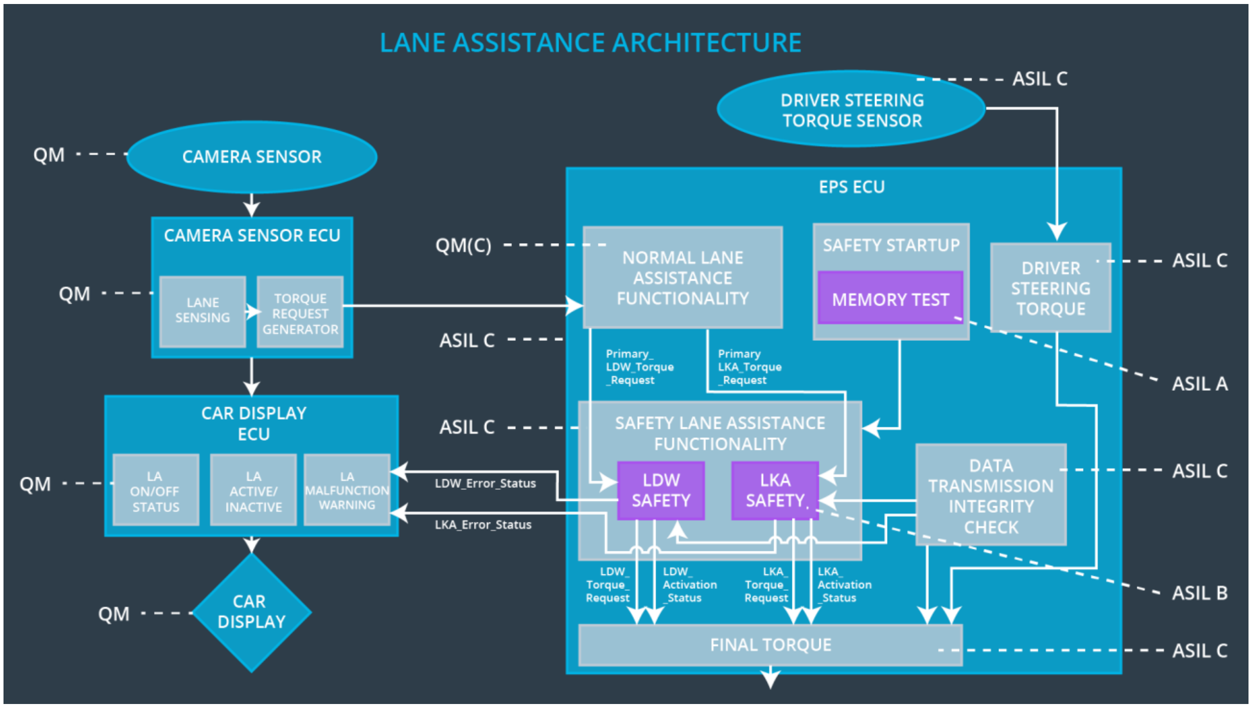
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the duration of the lane keeping assistance torque applied is less than Max_Duration	C	500 ms	LKA Safety block	Off
Technical Safety Requirement 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	C	500 ms	LKA Safety block	Off
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 zero.	C	500 ms	LKA Safety block	Off
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500 ms	Data Transmission Integrity Check	Off
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	Memory Test	Off

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

ID	Validation Acceptance Criteria	Verification Acceptance Criteria
Technical Safety Requirement 02-01-01	Validate that the Max_Duration is chosen from LKA validation acceptance criteria	Verify that the LKA is turned off if the assistant torque is applied for longer than MAX_Duration
Technical Safety Requirement 02-01-02	Validate that error_status_xxx message is sent to LKA_SAFETY_ACTIVATION when errors occur	Verify the LKA function is deactivated when error status received, and display ECU turns on warning light
Technical Safety Requirement 02-01-03	Validate a zero LKA_Torque_Request is sent to LKA_SAFETY_ACTIVATION as soon as a failure is detected by LKA	Verify the LKA_SAFETY_ACTIVATION receives a zero LKA_Torque_Request when a failure is detected
Technical Safety Requirement 02-01-04	Validate appropriate algorithms are chosen for checking validity and integrity of the data transmission	Verify the validity and integrity of data transmission for ‘LKA_Torque_Request’ signal is implemented
Technical Safety Requirement 02-01-05	Validate the algorithm used to test memory can detect any fault in memory	Verify memory test is conducted at start up of the EPS ECU

Refinement of the System Architecture

The refined system architecture is shown as following figure:



Allocation of Technical Safety Requirements to Architecture Elements

All Technical Safety Requirements have been 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	OFF	Oscillating torque frequency is higher than Max_Torque_Frequency or torque is higher than Max_Torque_Amplitude	Yes	Car Display
WDC-02	OFF	Lane keeping assistance torque is applied for more than Max_Duration	Yes	Car Display