Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2018-06-29

Document history

Date	Version	Editor	Description
2018-6-29	1.0	XU Kuangzheng	Initial Version
2018-6-29	2.0	XU Kuangzheng	Second Version

Table of Contents

Purpose of the Technical Safety Concept

The technical safety concept is a component level plan that defines both the architecture being implemented and the safety goals necessary to ensure the system satisfies ISO 26262.

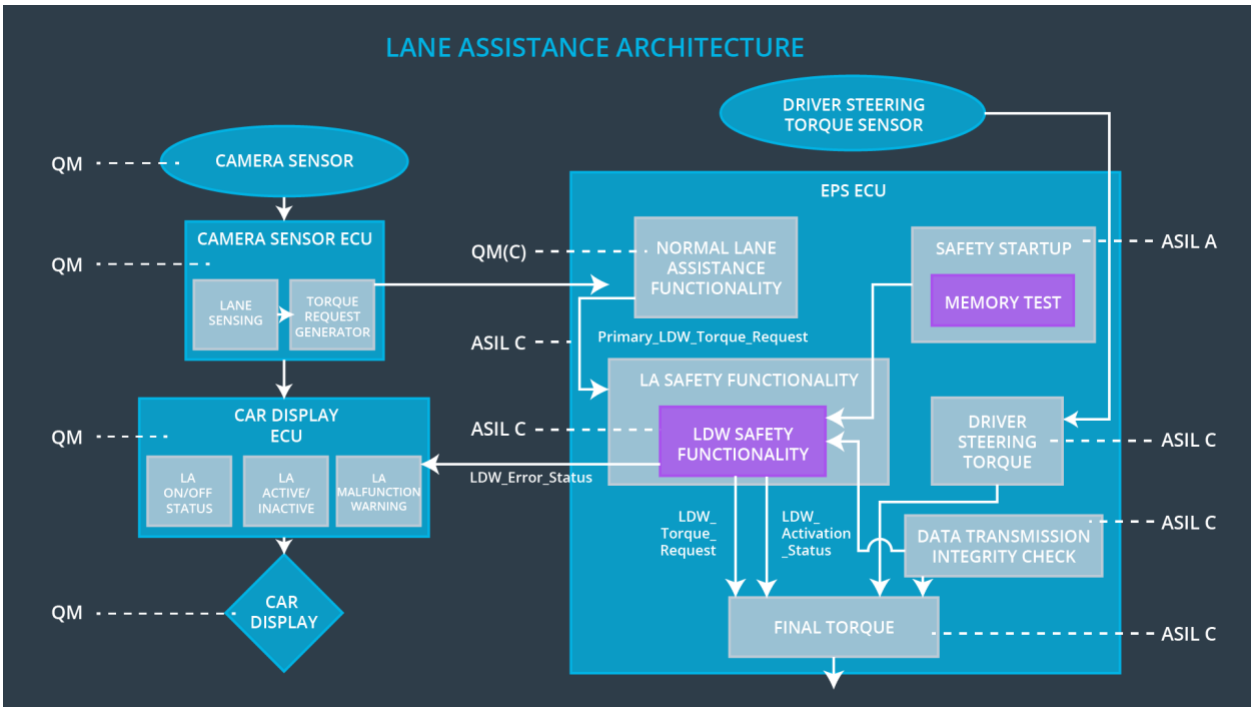
Inputs to the Technical Safety Concept

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	50MS	Set LDW system torque 0 and visual indication
Functional Safety Requirement 01-02	The electronic power steering subsystem shall ensure that the oscillating torque frequency is less than Max_Torque_Frequency	C	50MS	Set LDW system torque 0 and visual indication

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	500MS	LDW Disabled with visual indication

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

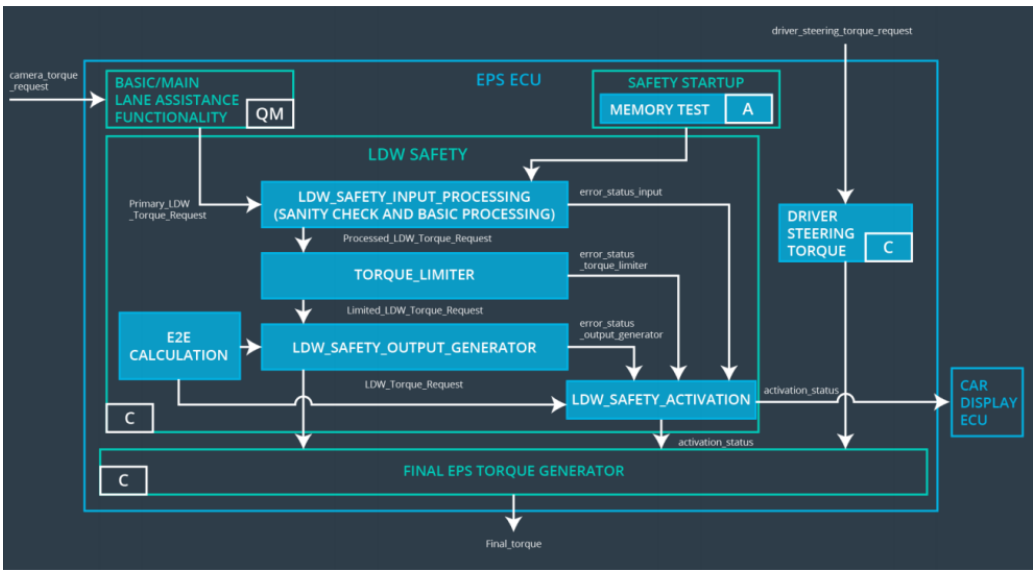
Element	Description
Camera Sensor	Camera device that retrieves images of the road in front of the vehicle.
Camera Sensor ECU - Lane Sensing	Detect the lane and check if the vehicle is moving away from the ego lane
Camera Sensor ECU - Torque request generator	Responsible for sending a torque request to the electronic power steering subsystem
Car Display	Graphic interface used to display the warning messages and setting changes.

Car Display ECU - Lane Assistance On/Off Status	Controlling a light that tells the driver if the lane 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	A sensor that measures that amount of effort the driver is making to steer the vehicle. This is important so that we do not interfere with intentional steering commands from the driver and impede his ability to control the vehicle.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Vibrates the steering wheel when vehicle is drifting away from the current lane unintentionally. Add appropriate amount of torque based on feedback from torque sensor to keep vehicle in current lane.
EPS ECU - Normal Lane Assistance Functionality	Process within the EPS ECU that manages the overall modes and state machine of the system
EPS ECU - Lane Departure Warning Safety Functionality	Process within the EPS ECU that checks the health of the LDW system and triggers any necessary safety modes
EPS ECU - Lane Keeping Assistant Safety Functionality	Process within the EPS ECU that checks the health of the LKA system and triggers any necessary safety modes
EPS ECU - Final Torque	Process within the EPS ECU that generates the final torque command
Motor	Actuator used to apply requested torque to 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 ms	LDW Safety	LDW torque set to 0
Technical Safety Requirement	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block	C	50 ms	LDW Safety	LDW torque set to 0

02	shall send a signal to the car display ECU to turn on a warning light.				
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	LDW torque 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	LDW torque 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	LDW Safety	LDW torque set to 0

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	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 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	C	50 ms	LDW Safety	LDW Disabled and torque set to 0

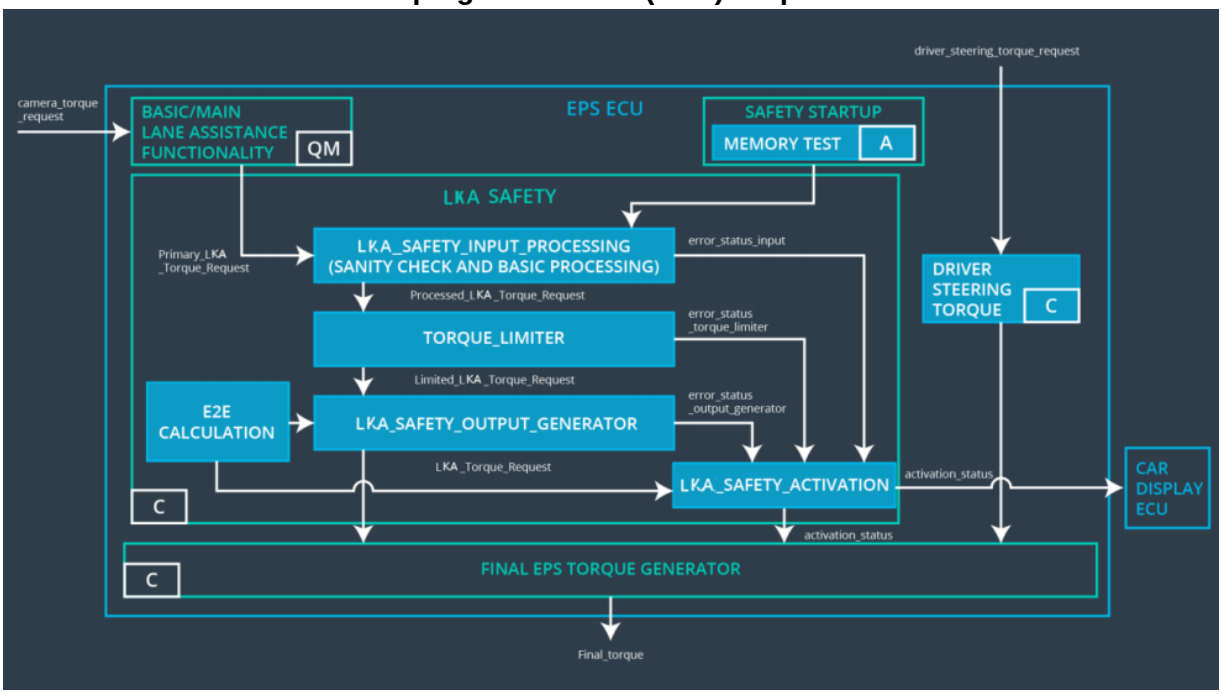
	'Max_Torque_Frequency.				
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light	C	50 ms	LDW Safety	OFF
Technical Safety Requirement 03	As soon as a failure is detected 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	LDW Disabled and torque set to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' ignal shall be ensured.	C	50 ms	Data Transmission Integrity Checking	LDW Disabled and torque set to 0
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	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 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 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 04	A tolerance window for 'LDW_Torque_Request' should be determined that keeps control stable	The actual command commanded torque should never deviate outside of that window of 'LDW_Torque_Request'

Technical Safety Requirement 05	Zero memory defects of any kind should be tolerated	Any memory defects found should disable lane keep system
Technical Safety Requirement 06	Validate that the Max_Torque_Frequency is chosen from LDW validation acceptance criteria	Verify that the frequency of the 'LDW_Torque_Request' sent is always below 'Max_Toque_Frequency'

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:

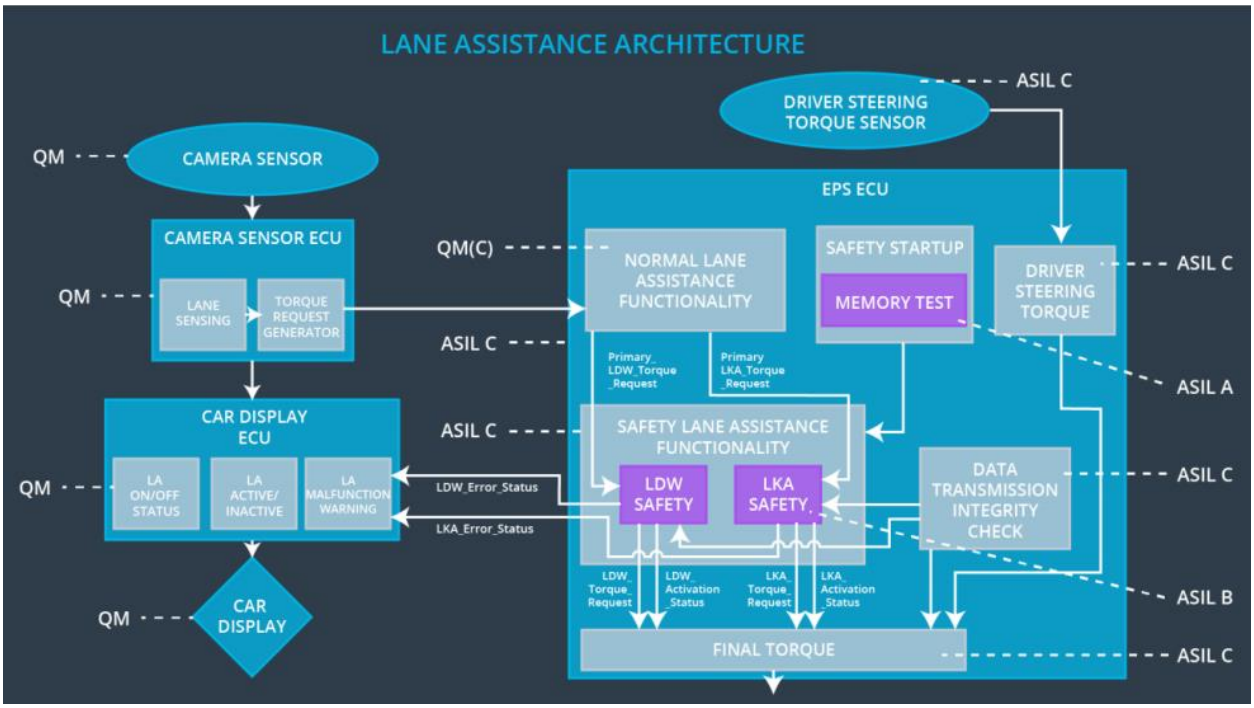
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall limit the duration of applied torque to ‘Max_Duration’.	B	500 ms	LKA Safety	OFF
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.	B	500 ms	LKA Safety	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.	B	500 ms	LKA Safety	OFF
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	LKA Safety	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	LDW Safety	OFF

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

ID	Validation Acceptance Criteria	Verification Acceptance Criteria
Technical Safety Requirement 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	Validate that error_status_xxx message is sent to LKA_SAFETY_ACTIVATION	Verify the LKA function is deactivated when error status received, and display ECU turns on warning light

02	when errors occur	
Technical Safety Requirement 03	Validate a zero LKA_Torque_Request is sent to LKA_SAFETY_ACTIVATION as soon as a failure is detected by LKA	Verify LKA_SAFETY_ACTIVATION receives a zero LKA_Torque_Request when a failure is detected
Technical Safety Requirement 04	A tolerance window for 'LDW_Torque_Request' should be determined that keeps control stable	The actual command commanded torque should never deviate outside of that window of 'LDW_Torque_Request'

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All Technical Safety Requirements are allocated to the Electronic Power Steering ECU.

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety	The lane keeping item shall ensure that the lane departure	X		

Requirement 01-01	oscillating torque amplitude is below Max_Torque_Amplitude			
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Disable LDW and alert	Oscillating torque frequency is higher than Max_Torque_Frequency or torque is higher than Max_Torque_Amplitude	YES	Driver indication of fault in LDW system
WDC-02	Disable LKA and alert	Lane keeping assistance torque is applied for more than Max_Duration	YES	Driver indication of fault in LKA system