Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
03/03/2019	V1.0	Madhu Hegde	First Version

Table of Contents

Document history

Table of Contents

Purpose of the Technical Safety Concept

Inputs to the Technical Safety Concept
- Functional Safety Requirements
- Refined System Architecture from Functional Safety Concept
  - Functional overview of architecture elements

Technical Safety Concept
- Technical Safety Requirements
- Refinement of the System Architecture
- Allocation of Technical Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to translate functional safety requirements established in the functional safety concept into technical safety requirements. This is an important step before realizing reliable software and hardware implementation.
The two aspects of technical safety concept are:

- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture

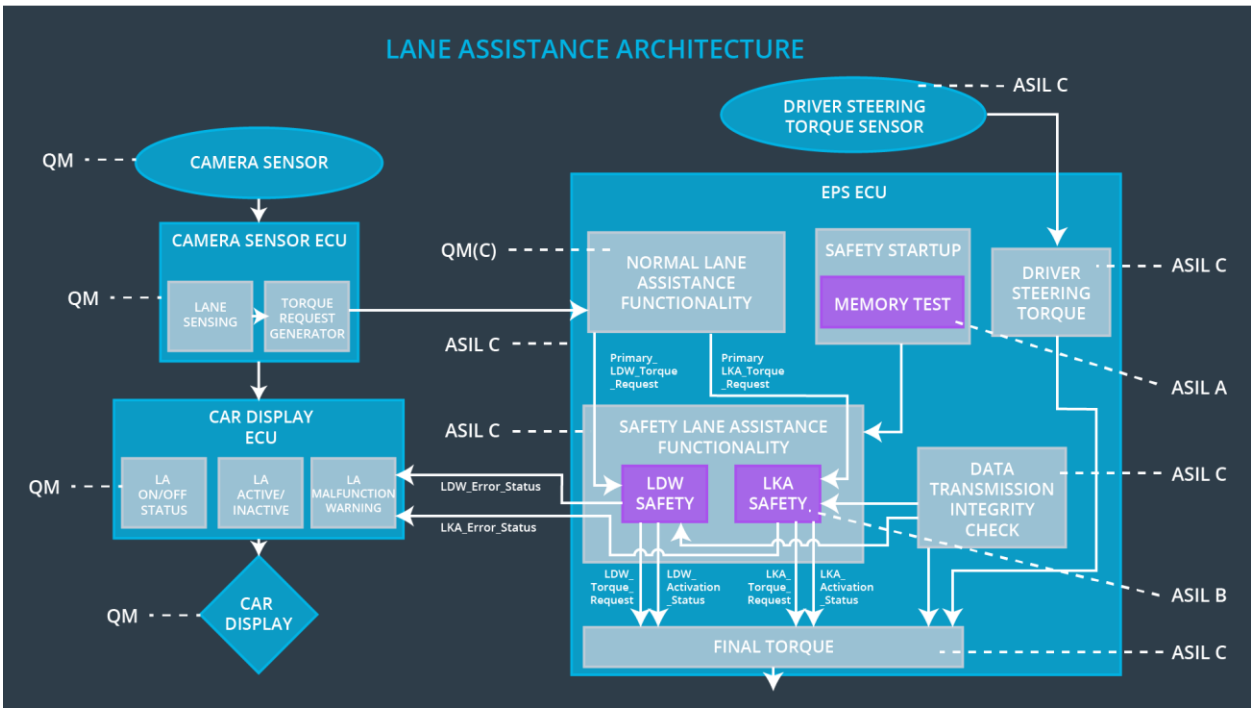
As a subsequent step, technical safety requirement will be considered within software and hardware implementation.

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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	B	500 ms	Lane Keeping Assistance torque is zero.

Refined System Architecture from Functional Safety Concept

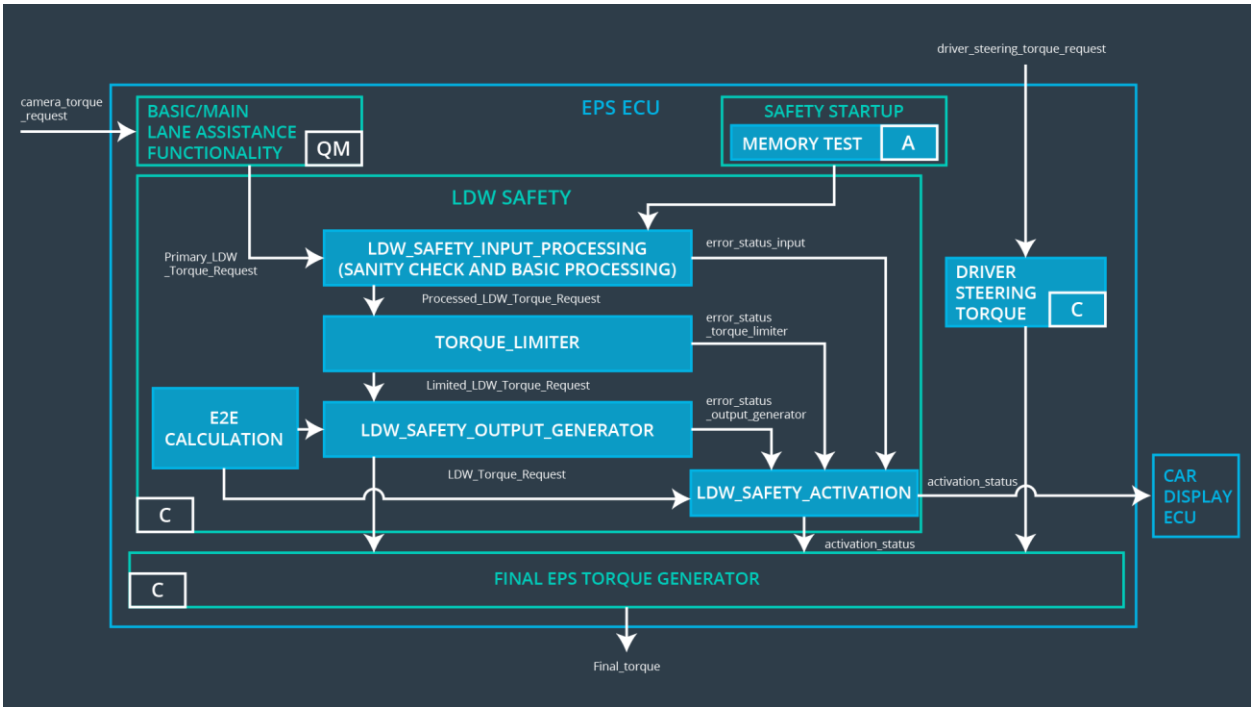


Functional overview of architecture elements

Element	Description
Camera Sensor	Captures front facing road images and sent to Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Lane sensing Software based on traditional Canny edge detection/Hough Transform or neural network based
Camera Sensor ECU - Torque request generator	Software module that estimates the torque based on vehicle location and lane detection to center the car in the middle of the lane. This adjustment

	torque is sent to Electronic Power Steering ECU.
Car Display	Provide visual feedback regarding warnings and display Lane Departure Assistance status. The display in Tesla also shows vehicles in other lanes.
Car Display ECU - Lane Assistance On/Off Status	Indicates status of Lane Assistance functionality (On/Off.)
Car Display ECU - Lane Assistant Active/Inactive	Indicate if Lane Assistance functionality is Active/Inactive
Car Display ECU - Lane Assistance malfunction warning	Indicates malfunction of Lane Assistance functionality.
Driver Steering Torque Sensor	Measures torque applied to the steering wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module receiving the driver's torque request from the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Software module receiving the Camera Sensor ECU torque request.
EPS ECU - Lane Departure Warning Safety Functionality	Software module ensuring the torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module ensuring the Lane Keeping Assistance functionality application is not activate more than Max_duration time.
EPS ECU - Final Torque	Combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the Motor.
Motor	Received final torque calculated by the Electronic Power Steering ECU and applies 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 Lane Departure Warning 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	Lane Departure Warning torque is zero.
Technical Safety Requirement 02	When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	Lane Departure Warning torque is zero.
Technical Safety Requirement 03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	Lane Departure Warning torque is zero.
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	Lane Departure Warning torque is zero.

Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque is zero.

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 Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Reques' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.'	C	50 ms	LDW Safety	LDW_Activation_Status is zero
Technical Safety Requirement 02	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall e set to zero.	C	50 ms	LDW Safety	LDW_Activation_Status is zero
Technical Safety	As soon as the LDW function deactivates the LDW feature, the	C	50 ms	LDW Safety	LDW_Activation_Status is zero

Requirement 03	'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.				
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Communication check	LDW_Activation_Status is zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in the mermory.	A	Ignition Cycle	Memory Test	LDW_Activation_Status is zero

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01	Validate the Max_Torque_Amplitude is the chosen from the Lane Departure Warning Validation	Verify Lane Departure Warning functionality is turned off.
Technical Safety Requirement 02	Validate the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LDW_SAFETY_ACTIVATION.	Verify Car Display ECU displays Lane Departure Warning malfunction warning signal.
Technical Safety Requirement 03	Validate the 'TORQUE_LIMITER' sends 'LDW_Torque_Request' with zero.	Verify Final EPS Torque generator receives LDW_Torque_Request of zero.
Technical Safety Requirement 04	Validate the 'TORQUE_LIMITER' calculate and sends the correct checksum and Awake counter for data transmission validity and integrity.	Verify functionality is turn off if there is a checksum or Awake counter discrepancy.
Technical Safety Requirement 5	Validate the Safety Startup Memory test to check memory faults catch memory faults.	Verify the Lane Departure Warning is turned off when the Safety Startup Memory fails.
Technical Safety Requirement 06	Validate the Max_Torque_Frequency set is the chosen from the Lane	Verify the functionality is turned off if the 'LDW_Torque_Request' frequency exceeds Max_Torque_Request.

	Departure Warning Acceptance Criteria.	

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 Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 02	When the Lane Keeping Assistance function deactivates, the 'LKA Safety' shall send a signal to the Car Display ECU to turn on a warning light.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement	When a failure is detected, the Lane Keeping Assistance function shall deactivate and the 'LKA_Torque_Request' shall be	C	500 ms	LKA Safety	Lane Keeping Assistance torque to

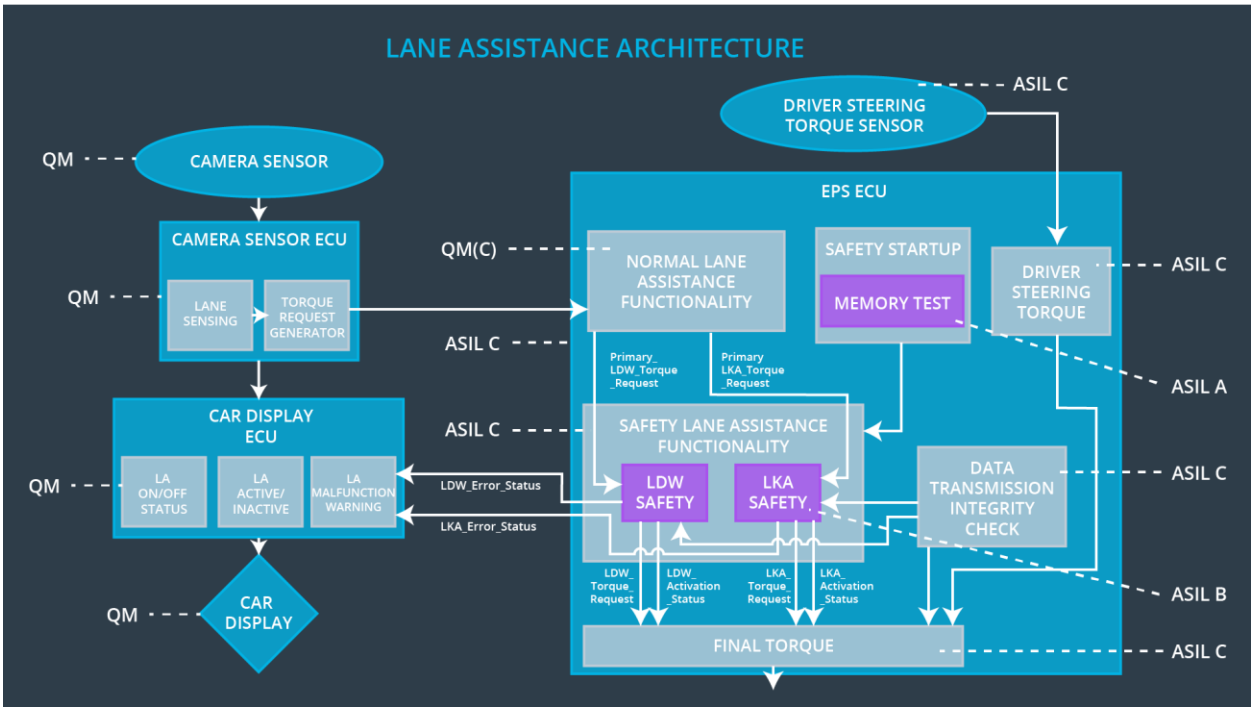
03	zero.				zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01	Validate the Max_Duration is set to the chosen value from LKA Validation Assistance Criteria	Verify that functionality is turned off after it is applied for Max_Duration.
Technical Safety Requirement 02	Validate the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LKA_SAFETY_ACTIVATION.	Verify that Car Display ECU displays the Lane Keeping Assistance malfunction warning signal.
Technical Safety Requirement 03	Validate the 'TORQUE_LIMITER' sends 'LKA_Torque_Request' with zero.	Verify that Final EPS Torque generator receives a LKA_Torque_Request of zero.
Technical Safety Requirement 04	Validate the 'TORQUE_LIMITER' calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity.	Verify that functionality is turn off if there is a CRC or Alive counter discrepancy.

Technical Safety Requirement 05	Validate the Safety Startup Memory test to check memory faults catch memory faults.	Verify that Lane Keeping Assistance is turned off when the Safety Startup Memory fails.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements were allocated to the Electronic Power Steering ECU. For the exact allocation within EPS ECU compare the technical requirement tables above.

Warning and Degradation Concept

Whenever there is system malfunction, lane assistance functions will be turned off and the driver will receive a warning light indication.

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning

WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_05	Yes	Lane Keeping Assistance Malfunction Warning on Car Display