Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 2.0

Document history

Date	Version	Editor	Description
Aug 20, 2017	1.0	Jian Liang Linn	Initial draft
Aug 22,2017	2.0	Jian Liang Linn	1) Changed architecture allocation of 01-01-04 to Data transmission integrity and 01-01-05 to Safety Block 2) Changed architecture allocation of 02-01-04 to Data transmission integrity and 02-01-05 to Safety Block 3) Added 01-02-02 technical safety requirment

Table of Contents

Purpose of the Technical Safety Concept

This document is to identify new requirements and define these hardware and software requirements to the system diagram for the lane assistance functional safety project as defined by ISO 26262 standard.

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 LKA function shall ensure that the lane departure oscillating torque amplitude is below MAX_TORQUE_AMPLITUDE	C	50 ms	Set vibration torque amplitude to zero
Functional Safety Requirement 01-02	The LKA function shall ensure that the lane departure oscillating torque frequency is below MAX_TORQUE_FREQUENCY	C	50 ms	Set vibration torque frequency to zero
Functional Safety Requirement 02-01	The EPS ECU shall ensure that the lane keeping assistance torque is applied for only MAX_DURATION	B	500 ms	Set lane keeping assistance torque to zero
Functional Safety Requirement 02-02	The EPS ECU shall ensure that the lane keeping assistance torque is set to zero when the Camera Sensor ECU stops detecting the lane and shall send the status (off) to the Car Display	B	500 ms	Set the lane keeping assistance torque to zero

Refined System Architecture from Functional Safety Concept

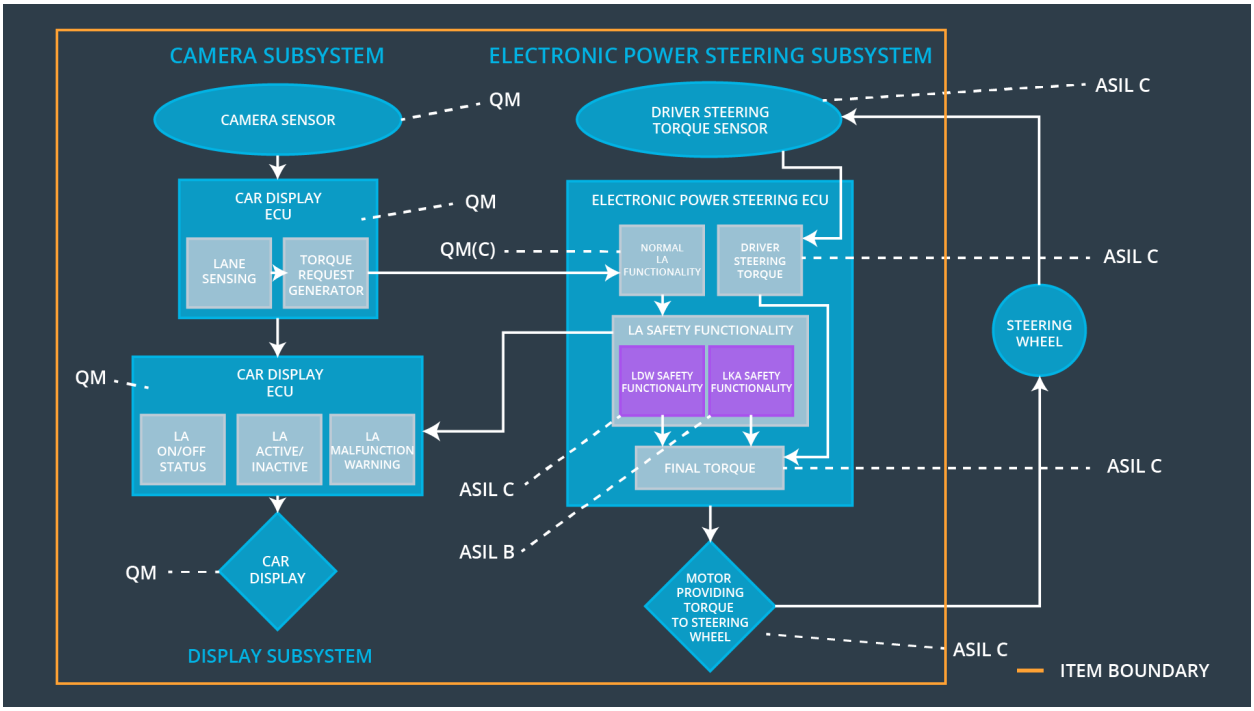

figure 1: Refined System Architecture

Functional overview of architecture elements

Element	Description
Camera Sensor	Sensor for capturing the videos of road conditions and lane lines
Camera Sensor ECU - Lane Sensing	Detecting the lane lines and determining when the vehicle leaves the lane
Camera Sensor ECU - Torque request generator	Calculating and sending the additional torque for the LDW and LKA functions
Car Display	Display for warning and activation/deactivation of LDW and LKA functions

Car Display ECU - Lane Assistance On/Off Status	Displaying the warning LDW and LKA on/off status
Car Display ECU - Lane Assistant Active/Inactive	Displaying the warning of LDW and LKA activation/deactivation status
Car Display ECU - Lane Assistance malfunction warning	Displaying the warning of LDW and LKA malfunctions
Driver Steering Torque Sensor	Responsible for measuring how much steering torque the driver applies to the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Module responsible for receiving the Camera Sensor ECU torque request
EPS ECU - Normal Lane Assistance Functionality	Responsible for receiving the driver steering torque sensor input
EPS ECU - Lane Departure Warning Safety Functionality	Responsible for keeping the lane departure oscillating torque amplitude and frequency below the MAX_TORQUE_AMPLITUDE and MAX_TORQUE_FREQUENCY
EPS ECU - Lane Keeping Assistant Safety Functionality	Responsible for ensuring the LKA torque does not exceed MAX_DURATION and when the lane detection has lost, it is deactivated
EPS ECU - Final Torque	Responsible for ensuring LDW, LKA and the driver steering torque requests are combined and are sent to the Motor
Motor	Responsible to apply requested torque to the steering by EPS ECU for LKA and LDW functions

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	Camera ECU	Car Display ECU

		Steering 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		

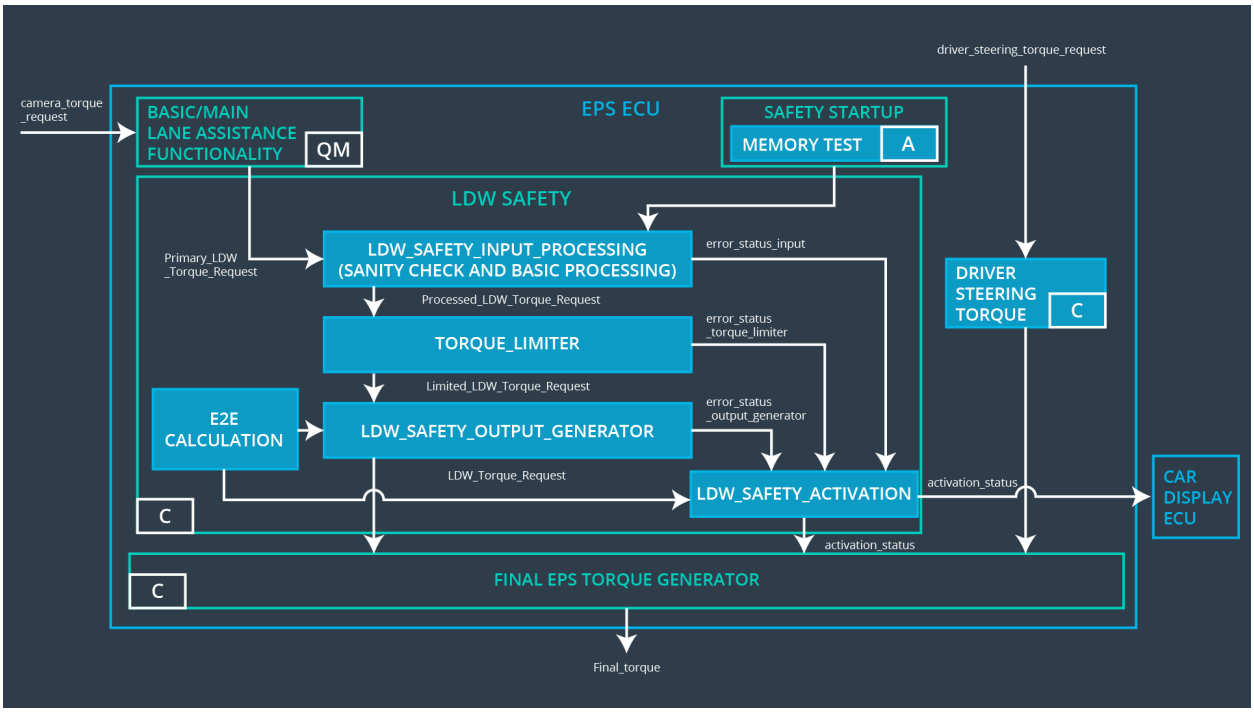

figure 2: Technical Safety Requirements

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 01-01-01	The LDW safety component shall ensure the torque amplitude of the LDW_TORQUE_REQUEST sent to the EPS Torque component is below MAX_TORQUE_AMPLITUDE	C	50 ms	LDW Safety	Set lane departure warning torque to zero

Technical Safety Requirement 01-01-02	The LDW Safety Software shall send a signal to the Car Display ECU to turn on a warning light when the LDW function detect a failure	C	50 ms	LDW Safety	Set lane departure warning torque to zero
Technical Safety Requirement 01-01-03	The LDW feature is deactivated when the LDW function detects a failure and the LDW_TORQUE_REQUEST shall be set to zero	C	50 ms	LDW Saftey	Set lane departure warning torque to zero
Technical Safety Requirement 01-01-04	The LDW_TORQUE_REQUEST data signal validity and integrity shall be ensured	C	50 ms	Data transmission integrity	Set lane departure warning toque to zero
Technical Safety Requirement 01-01-05	Any memory faults test shall be conducted at the startup of the EPS ECU	A	Ignition cycle	Safety Block	Set lane departure warning to 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	ASI	Fault Tolerant Time	Architecture Allocation	Safe State

		L	Interval		
Technical Safety Requirement 01-02-01	The torque frequency request that sent to EPS Torque component shall be ensured below the MAX_TORQUE_FREQUENCY	C	50 ms	LDW Safety	Set lane departure warning torque to zero
Technical Safety Requirement 01-02-02	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the LDW_Torque_Frequency_Request shall be set to zero	C	50 ms	LDW Safety	Set lane departure warning torque to zero

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

ID	Validation Acceptance Criteria	Verification Acceptance Criteria
Technical Safety Requirement 01-01-01	Validate the MAX_TORQUE_AMPLITUDE is set as chosen from LDW validation acceptance criteria	Verify the system turns off if the lane departure warning the LDW_TORQUE_REQUEST value exceeds the MAX_TORQUE_AMPLITUDE
Technical Safety Requirement 01-01-02	Validate the TORQUE_LIMITER sends error_status_torque_limiter signal to the LDW_SAFETY_ACTIVATION	Verify the Car Display ECU displays the LDW malfunction warning light.
Technical Safety Requirement 01-01-03	Validate the TORQUE_LIMITER sends a zero LDW_TORQUE_REQUEST	Verify the Final EPS Torque Generator receive zero LDW_TORQUE_REQUEST
Technical Safety Requirement 01-01-04	Validate the TORQUE_LIMITER calculate and sends a correct CRC for data signal transmission validity and integrity	Verify the system turns off if the lane departure warning LDW_TORQUE_REQUEST data signal has invalid CRC

Technical Safety Requirement 01-01-05	Validate startup memory test to check memory faults	Verify the system turns off if the startup memory test fails
Technical Safety Requirement 02-01-01	Validate MAX_TORQE_FREQUENCY is set as chosen from LDW validation acceptance criteria	Verify the system turns off if the lane departure warning LDW_TORQUE_REQUEST exceeds the MAX_TORQUE_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 02-01-01	The LKA shall ensure the duration of the lane keeping assistance torque applied is less than MAX_DURATION	C	500 ms	LKA Safety	Set the lane keeping assistance torque to zero
Technical Safety	The LKA software shall send a signal to the Car Display ECU to	C	500 ms	LKA Safety	Set the lane keeping

Requirement 02-01-02	turn of the warning light when LKA function deactivate the lane keeping assistance feature				assistance torque to zero
Technical Safety Requirement 02-01-03	The LKA software shall deactivate the lane keeping assistance feature and LKA_TORQUE_REQUEST to be set to zero when a failure is detected	C	500 ms	LKA Safety	Set the lane keeping assistance torque to zero
Technical Safety Requirement 02-01-04	LKA_TORQUE_REQUEST data signal validity and integrity shall be ensured	C	500 ms	Data transmission integrity	Set the lane keeping assistance torque to zero
Technical Safety Requirement 02-01-05	Any memory faults test shall be conducted at the startup of the EPS ECU	A	Ignition cycle	Safety Block	Se the lane keeping assistance torque to zero

Functional Safety Requirement 02-02 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 02-02	The EPS ECU shall ensure the lane keeping assistance torque is set to zero when the Camera Sensor ECU stops detecting the lane and sends the status to the Car Display	X		

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

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State

Technical Safety Requirement 02-02-01	The LKA shall ensure the loss of the camera sensor torque request transmission deactivates the LKA function and LKA_TORQUE_REQUEST shall be set to zero	C	500 ms	LKA Safety	Set the lane keeping assistance torque to zero

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

ID	Validation Acceptance Criteria	Verification Acceptance Criteria
Technical Safety Requirement 02-01-01	Validate the MAX_DURATION is set as chosen from LKA validation acceptance criteria	Verify the system turns off if the lane departure warning the LKA_TORQUE_REQUEST value exceeds the MAX_DURATION
Technical Safety Requirement 02-01-02	Validate the TORQUE_LIMITER sends error_status_torque_limiter signal to the LKA_SAFETY_ACTIVATION	Verify the Car Display ECU displays the LKA malfunction warning light.
Technical Safety Requirement 02-01-03	Validate the TORQUE_LIMITER sends a zero LKA_TORQUE_REQUEST	Verify the Final EPS Torque Generator receive zero LKA_TORQUE_REQUEST
Technical Safety Requirement 02-01-04	Validate the TORQUE_LIMITER calculate and sends a correct CRC for data signal transmission validity and integrity	Verify the system turns off if the lane departure warning LKA_TORQUE_REQUEST data signal has invalid CRC
Technical Safety Requirement 02-01-05	Validate startup memory test to check memory faults	Verify the system turns off if the startup memory test fails

Technical Safety Requirement 02-02-01	Validate the Camera ECU sends zero LKA_TORQUE_REQUEST when failing to detect the lane and there is invalid data transmission	Verify the system turns off if the lane departure warning LKA_TORQUE_REQUEST has invalid CRC from the Camera ECU

Refinement of the System Architecture

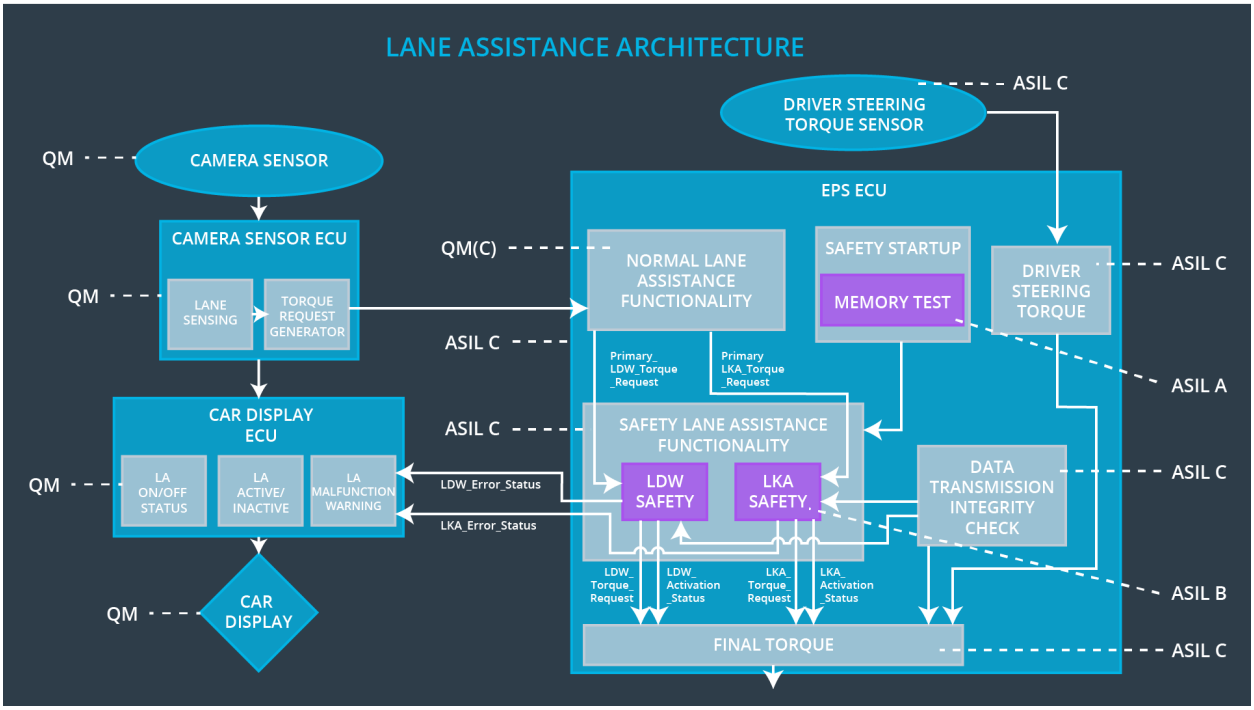

figure 3: Refined System Architecture

Allocation of Technical Safety Requirements to Architecture Elements

The table below summarizes the identified the requirements from Technical Safety Requirements section and all the requirements have been allocated to EPS ECU.

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU

Technical Safety Requirement 01-01-01	The LDW shall ensure the amplitude of the LDW_TORQUE_REQUEST sent to EPS torque is below MAX_TORQUE_AMPLITUDE	X		
Technical Safety Requirement 01-01-02	The LDW shall send a data signal to the Car Display ECU to turn on a warning light when it deactivates the LDW function	X		
Technical Safety Requirement 01-01-03	The LDW shall deactivate the LDW function and the LDW_TORQUE_REQUEST signal shall be set to zero when a failure is detected	X		
Technical Safety Requirement 01-01-04	The LDW_TORQUE_REQUEST data signal transmission validity and integrity shall be ensured	X		
Technical Safety Requirement 01-01-05	Any memory failures shall be tested at the startup of EPS ECU	X		
Technical Safety Requirement 01-02-01	The LDW shall ensure the frequency of the LDW_TORQUE_REQUEST sent to EPS ECU is below MAX_TORQUE_FREQUENCY	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State Invoked	Driver Warning
Warning Degradation 01-01	Turn off LDW function	Malfunction_01, Malfunction_02	LDW torque shall be set to zero	Lane Keeping Assistance function inactive and Malfunction

				warning is set in the Car Display ECU
Warning Degradation 01-02	Turn off LKA function	Malfunction_04, Malfunction _05	LKA torque shall be set to zero	Lane Keeping Assistance function inactive and Malfunction warning is set in the Car Display ECU