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
10/23/2018	1.0	Yan Cui	First draft
11/01/2018	1.1	Yan Cui	Revision for submission
11/03/2018	2.0	Yan Cui	Revised based on review feedback
11/04/2018	3.0	Yan Cui	Revised one table based on review feedback

Table of Contents

Purpose of the Technical Safety Concept

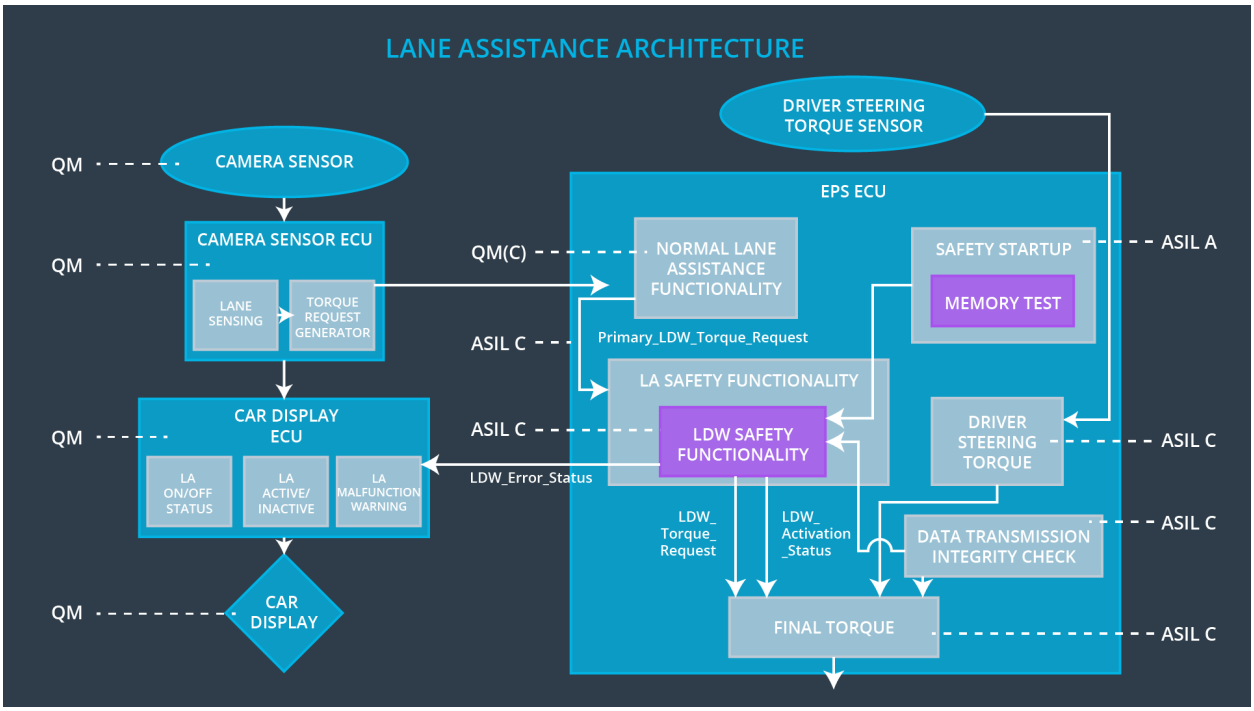
In this document, new requirements are assigned to the system architecture. The technical safety concept covered in this document is more concrete and gets into the details of the item's technology.

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 EPS ECU shall ensure that the lane departure warning torque amplitude is below is Max_Torque_Amplitude	C	50ms	Oscillating torque amplitude below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The EPS ECU shall ensure that the lane departure warning torque frequency is below is Max_Torque_Frequency	C	50ms	Oscillating torque frequency below Max_Torque_Frequency
Functional Safety Requirement 01-03	Lane Departure Warning (LDW) function shall be deactivated the time when camera sensor stops working	C	10ms	LDW is deactivated
Functional Safety Requirement 02-01	The electronic power steering ECU needs to ensure that Lane Keeping Assistance torque is applied only Max_Duration	B	500ms	Lane Keeping Assistance torque is zero
Functional Safety Requirement 02-02	The Lane Keeping Assistance (LKA) shall be deactivated the time when camera sensor stops working	D	10ms	Function is deactivated

Refined System Architecture from Functional Safety Concept



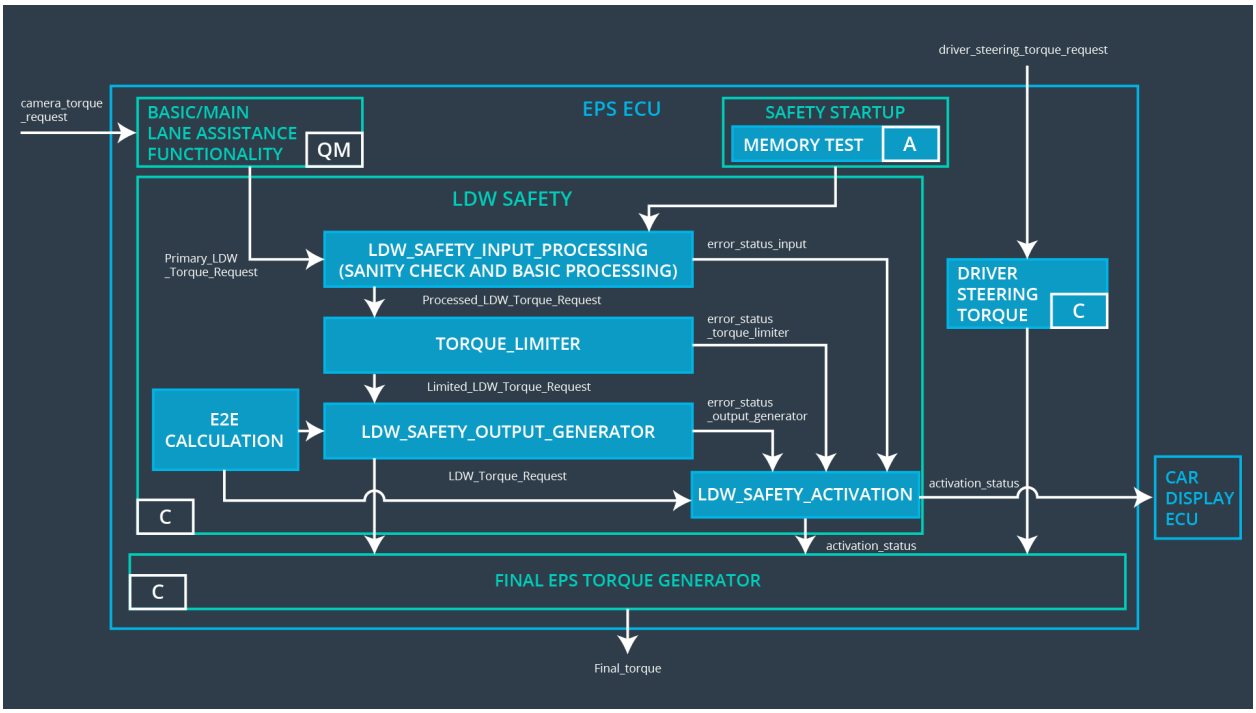
Functional overview of architecture elements

Element	Description
Camera Sensor	Capture road images and feed them to Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Software module, detect the lane line position from images captured by Camera Sensor.
Camera Sensor ECU - Torque request generator	Software module, calculate the torque to be requested to Electronic Power Steering ECU.
Car Display	Display warnings to driver.
Car Display ECU - Lane Assistance On/Off Status	Indicate status of the Lane Assistance function On/Off.
Car Display ECU - Lane Assistant Active/Inactive	Indicate function status of Lane Assistant, Active/Inactive.
Car Display ECU - Lane Assistance malfunction warning	Indicate malfunction on the Lane Assistance function.
Driver Steering Torque Sensor	Measure the torque applied to steering wheel by the driver.

Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module, receive driver's steering torque request from the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Software module, receive Camera Sensor ECU torque request.
EPS ECU - Lane Departure Warning Safety Functionality	Software module, make sure the torque applied having amplitude within the limited range.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module, make sure the LKA function is not active more than Max_Duration time.
EPS ECU - Final Torque	Combine the torque request from LKA and LDW functions, and send torque to Motor.
Motor	Physically applies torque to steering wheels.

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 EPS ECU shall ensure that the lane departure warning torque amplitude is below is 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 needs to ensure the amplitude of the LDW torque request being sent to Electronic Power Steering torque is below Max_Torque_Amplitude.	C	50ms	LDW Safety	LDW torque at zero
Technical Safety Requirement 02	When the Lane Departure Warning is deactivated, the LDW Safety module must send a signal message to Car Display ECU indicating the warning.	C	50ms	LDW Safety	LDW torque at zero
Technical Safety Requirement 03	When failure of Lane Departure Warning function is detected, it must deactivate the LDW feature and reset torque request to zero.	C	50ms	LDW Safety	LDW torque at zero
Technical Safety Requirement 04	The validity and integrity of data transmission of LDW torque request needs to be ensured.	C	50ms	Data transmission integrity check	LDW torque at zero

Technical Safety Requirement 05	Memory test needs to be conducted at starting of EPS ECU to check any memory issue.	A	Ignition cycle	Safety startup - Memory test	LDW torque at 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 EPS ECU shall ensure that the lane departure warning torque frequency is below is Max_Torque_Frequency	X	LDW Safety	LDW torque at zero

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 must ensure the torque frequency sent to Electronic Power Steering Torque is below Max_Torque_Frequency.	C	50ms	LDW Safety	LDW torque at zero
Technical Safety Requirement 02	When the Lane Departure Warning is deactivated, the LDW Safety module must send a signal message to Car Display ECU indicating the warning.	C	50ms	LDW Safety	LDW torque at zero
Technical Safety Requirement 03	When failure of Lane Departure Warning function is detected, it must deactivate the LDW feature and reset torque request to zero.	C	50ms	LDW Safety	LDW torque at zero

Technical Safety Requirement 04	The validity and integrity of data transmission of LDW torque request needs to be ensured.	C	50ms	Data transmission integrity check	LDW torque at zero
Technical Safety Requirement 05	Memory test needs to be conducted at starting of EPS ECU to check any memory issue.	A	Ignition cycle	Safety startup - Memory test	LDW torque at zero

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

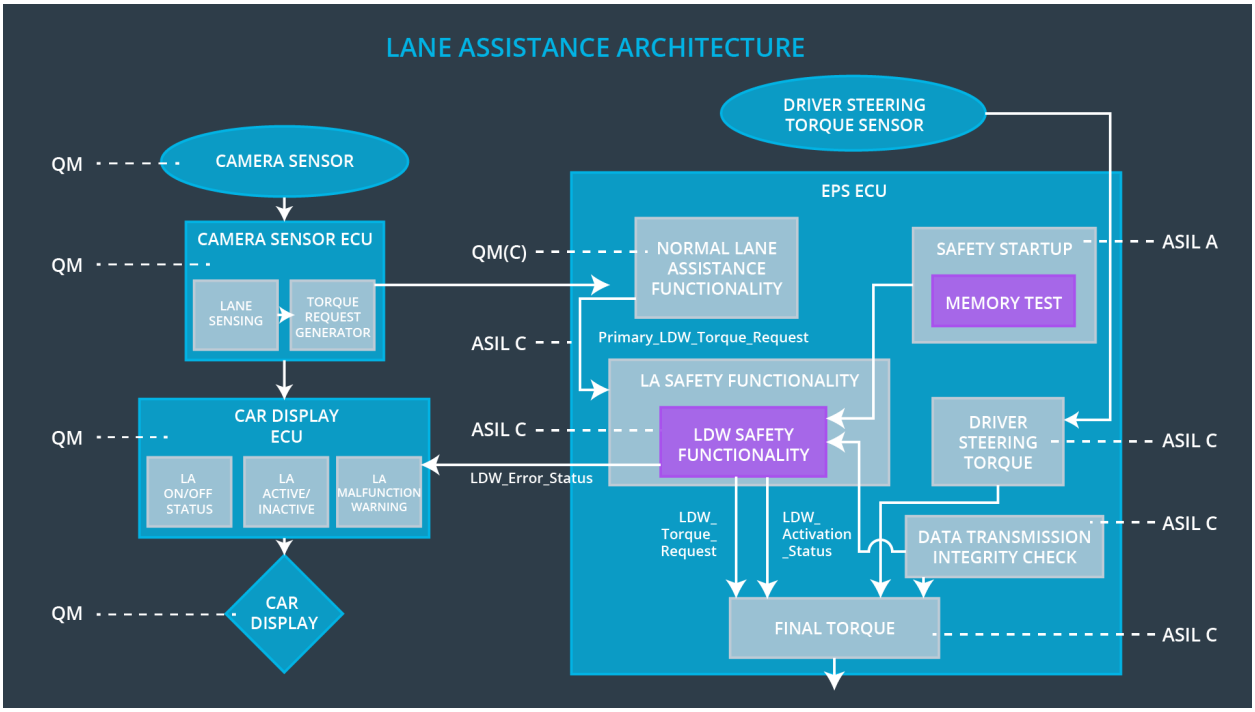
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 must make sure the duration of the LKA torque is activated within time of Max_Duration.	B	500ms	LKA Safety	LKA torque at zero.
Technical Safety Requirement 02	When Lane Keeping Assistance function is deactivated, the LKA safety component must send a signal message to Car Display ECU, indicating a warning.	B	500ms	LKA Safety	LKA torque at zero.

Technical Safety Requirement 03	When failure is detected, the Lane Keeping Assistance function must be deactivated and the corresponding torque request must be reset to zero.	B	500ms	LKA Safety	LKA torque at zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for LKA torque request must be ensured.	B	500ms	Data transmission integrity check	LKA torque at zero.
Technical Safety Requirement 05	Memory test must be conducted at starting of EPS ECU to check any memory issue.	A	Ignition cycle	Safety startup - Memory test	LKA torque at zero.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	Technical Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	The Lane Departure Warning safety component needs to ensure the amplitude of the LDW torque request being sent to Electronic Power Steering torque is below Max_Torque_Amplitude.	X		
Technical Safety Requirement 01-01-02	When the Lane Departure Warning is deactivated, the LDW Safety module must send a signal message to Car Display ECU indicating the warning.	X		
Technical Safety Requirement 01-01-03	When failure of Lane Departure Warning function is detected, it must deactivate the LDW feature and reset torque request to zero.	X		
Technical Safety Requirement 01-01-04	The validity and integrity of data transmission of LDW torque request needs to be ensured.	X		
Technical Safety Requirement 01-01-05	Memory test needs to be conducted at starting of EPS ECU to check any memory issue.	X		
Technical Safety Requirement 02-01-01	The Lane Keeping Assistance safety component must make sure the duration of the LKA torque is activated within time of Max_Duration.	X		
Technical Safety Requirement 02-01-02	When Lane Keeping Assistance function is deactivated, the LKA safety component must send a signal message to Car Display ECU, indicating a warning.	X		

Technical Safety Requirement 02-01-03	When failure is detected, the Lane Keeping Assistance function must be deactivated and the corresponding torque request must be reset to zero.	X		
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for LKA torque request must be ensured.	X		
Technical Safety Requirement 02-01-05	Memory test must be conducted at starting of EPS ECU to check any memory issue.	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning (LDW) function	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Lane Departure Warning (LDW) malfunction warning on Car Display
WDC-02	Turn off Lane Keeping Assistance (LKA) function	Malfunction_03, Malfunction_05	Yes	Lane Keeping Assistance (LKA) malfunction warning on Car Display