Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version:1.0

Document history

Date	Version	Editor	Description
11/2/17	1.0	Avnit Mackin	First attempt

Table of Contents

Purpose of the Technical Safety Concept

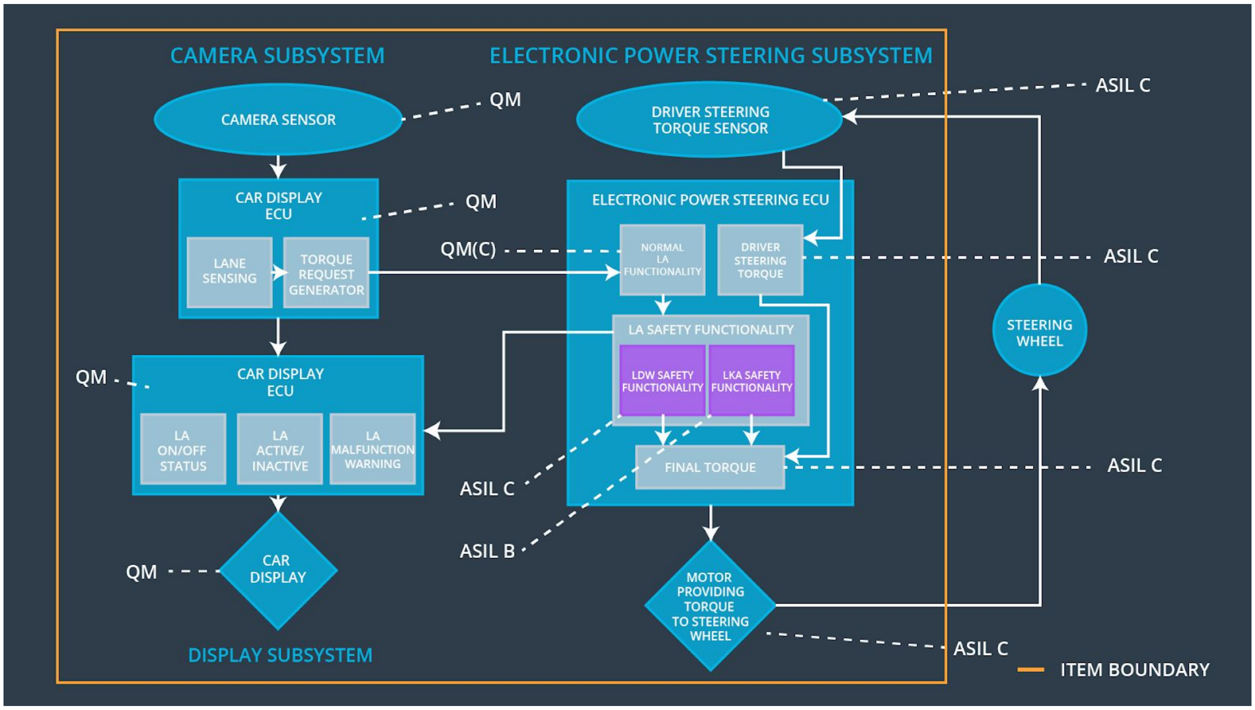
The Technical Safety Concept defines how the subsystems interact at the message level and describes how the ECU's communicate with each other.

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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	LDW shall set the oscillating torque amplitude to 0
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	LDW shall set the oscillating torque amplitude to 0
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	The functionality will be turned off.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	The Camera Sensor reads in images from the road.
Camera Sensor ECU - Lane Sensing	The Camera Sensor ECU- Lane Sensing identifies when the vehicle accidently departed its lane.
Camera Sensor ECU - Torque request generator	The Camera Sensor ECU - Torque request generator sends the appropriate messages to Car Display ECU and the Electronic Power Steering ECU.
Car Display	The Car Display display the lane assistance status to the driver (On/Off/Active/Inactive).
Car Display ECU - Lane Assistance On/Off Status	The Car Display display ECU sends the appropriate lane assistance On/Off status messages to Car Display.
Car Display ECU - Lane Assistant	The Car Display display ECU sends the appropriate lane assistant Active/Inactive

Active/Inactive	status messages to Car Display.
Car Display ECU - Lane Assistance malfunction warning	The Car Display display ECU sends the appropriate lane assistant malfunction warning status messages to Car Display.
Driver Steering Torque Sensor	Detect the driver steering torque.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Analyzes driver steering torque
EPS ECU - Normal Lane Assistance Functionality	Responsible for the Normal Lane Assistance Functionality
EPS ECU - Lane Departure Warning Safety Functionality	Responsible for the Lane Departure Warning Safety Functionality
EPS ECU - Lane Keeping Assistant Safety Functionality	Responsible for the Lane Keeping Assistant Safety Functionality
EPS ECU - Final Torque	Gives the final Electronic Power Steering torque output.
Motor	Provides torque 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 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 output is set to zero
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	LDW torque output is set to zero
Technical Safety Requirement	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the	C	50 ms	LDW Safety	LDW torque output is set to zero

03	'LDW_Torque_Request' shall be set to zero.				
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 Check	LDW torque output is set to zero
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	Safety startup - Memory test	LDW torque output is set 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	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 'Max_Torque_Frequency.	C	50 ms	LDW Safety	LDW torque output is set to zero
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	LDW torque output is set to zero
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 output is set to zero
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 Check	LDW torque output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	50 ms	Ignition Cycle	LDW torque output is set to zero

Lane Keeping Assistance (LKA) Requirements:

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

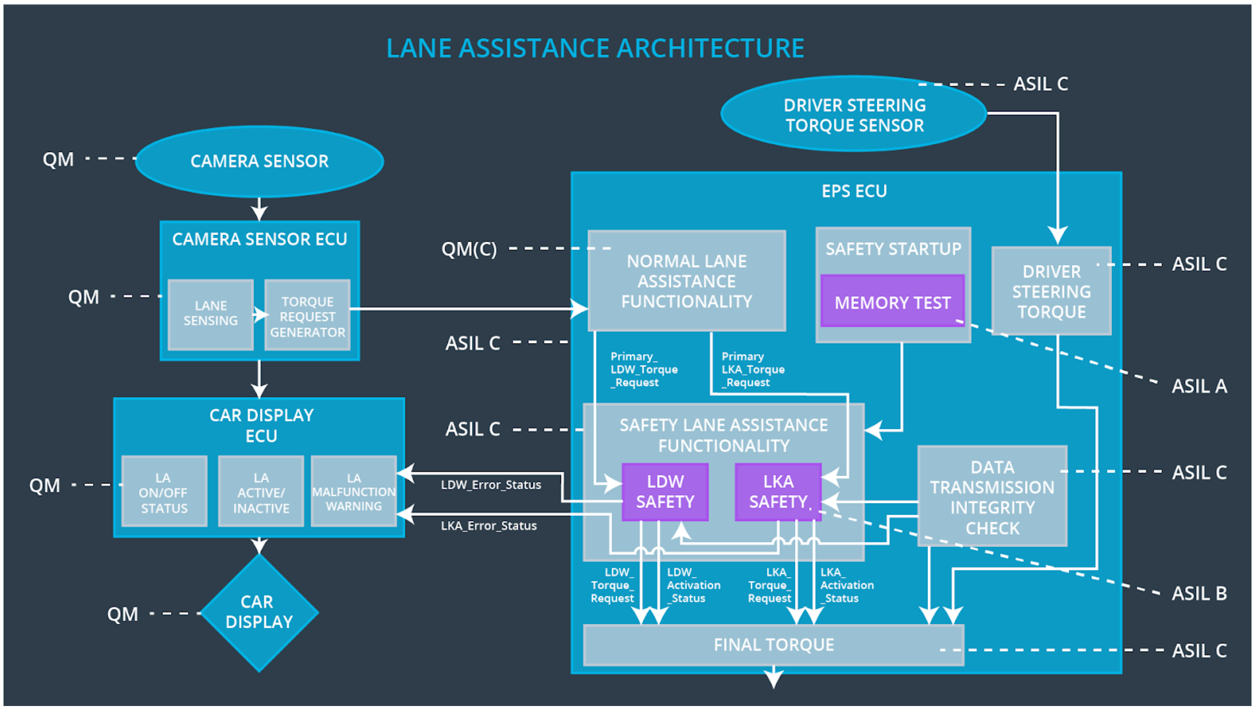
ID	**Functional Safety Requirement**	**Electronic Power Steering ECU**	**Camera ECU**	**Car Display ECU**
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 LKA safety component shall ensure duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is only for Max_Duration.	B	500 ms	LKA Safety Block	LKA torque output is set to zero
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 Block	LKA torque output is set to zero
Technical	As soon as a failure is	B	500 ms	LKA Safety Block	LKA torque

Safety Requirement 03	detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero				output is set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data Transmission Integrity Check	LKA torque output is set to zero
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	Safety startup - Memory test	LKA torque output is set to zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU.