Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12-25-2018	1.0	Eduardo Paz	Initial release

Table of Contents

Purpose of the Technical Safety Concept

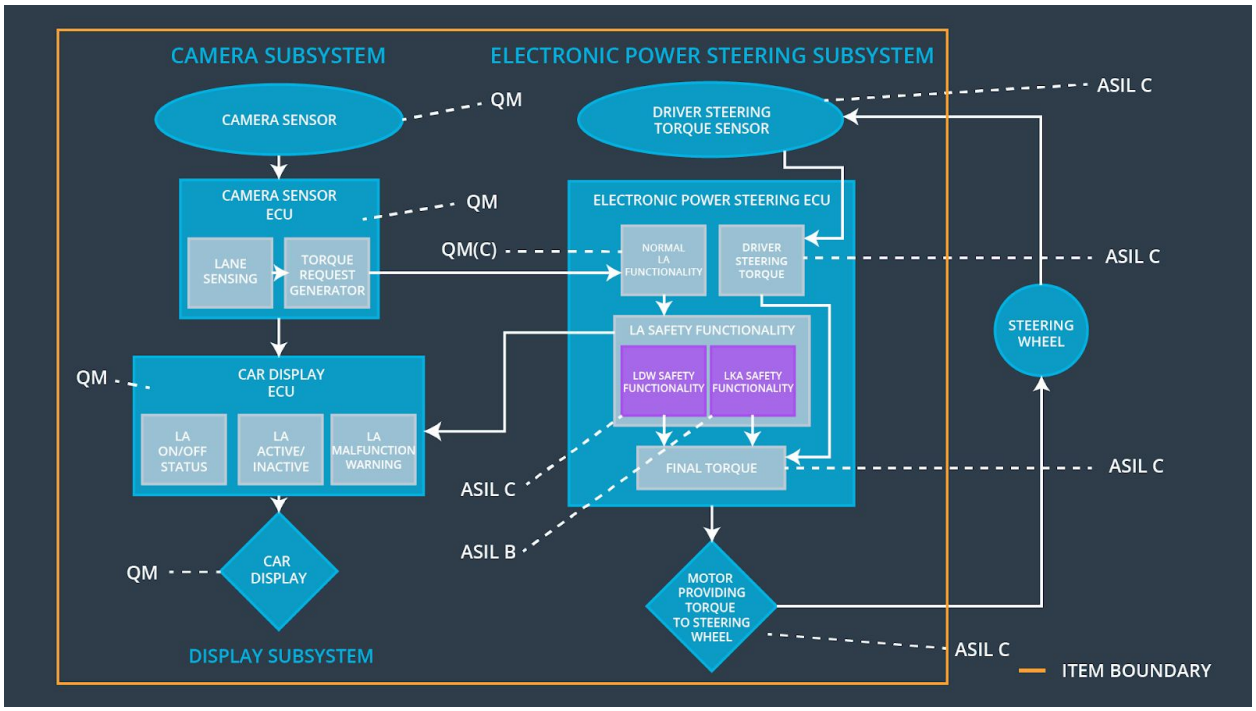
The Technical Safety Concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

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 Electronic Power Steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	LDW oscillating amplitude is set to 0
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	LDW oscillating frequency is set to 0
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	LKA is turned off

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Reads in images from the road
Camera Sensor ECU - Lane Sensing	Identifies when the vehicle has departed its lane, and sends appropriate messages to “Camera Sensor ECU”
Camera Sensor ECU - Torque request generator	Sends torque requests to “EPS ECU”
Car Display	Displays useful information to the driver
Car Display ECU - Lane Assistance On/Off Status	Shows if the Lane Assistance function is on/off
Car Display ECU - Lane Assistant Active/Inactive	Shows is Lane Assistant function is active/inactive
Car Display ECU - Lane Assistance malfunction warning	Shows warnings of the Lane Assistance function
Driver Steering Torque Sensor	Monitors how much torque is applied to the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Decides how much torque will be applied depending on the “Driver Steering Torque Sensor” information
EPS ECU - Normal Lane Assistance Functionality	Receives torque requests
EPS ECU - Lane Departure Warning Safety Functionality	Checks LDW Safety functionality
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks LKA Safety functionality
EPS ECU - Final Torque	Decides the final torque to the steering wheel
Motor	Steers the 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	‘EPS ECU - LDW Safety’ software block	‘LDW_Torque_Request’ set to 0
Technical Safety	As soon as the LDW function deactivates the	C	50 ms	‘EPS ECU - LDW Safety’	‘LDW_Torque_Request’ set to 0

Requirement 02	LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.			software block	
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	‘EPS ECU - LDW Safety’ software block	‘LDW_Torque_Request’ 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	‘Data Transmission Integrity Check’	N/A
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’	‘LDW_Torque_Request’ 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 'Max_Torque_Frequency'.	C	50 ms	'EPS ECU - LDW Safety' software block	'LDW_Torque_Request' set to 0
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	'EPS ECU - LDW Safety' software block	'LDW_Torque_Request' set to 0
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	'EPS ECU - LDW Safety' software block	'LDW_Torque_Request' 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	'Data Transmission Integrity Check'	'LDW_Torque_Request' set to 0
Technical Safety Requirement	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	'Safety Startup'	'LDW_Torque_Request' set to

05					0

Lane Keeping Assistance (LKA) Requirements:

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

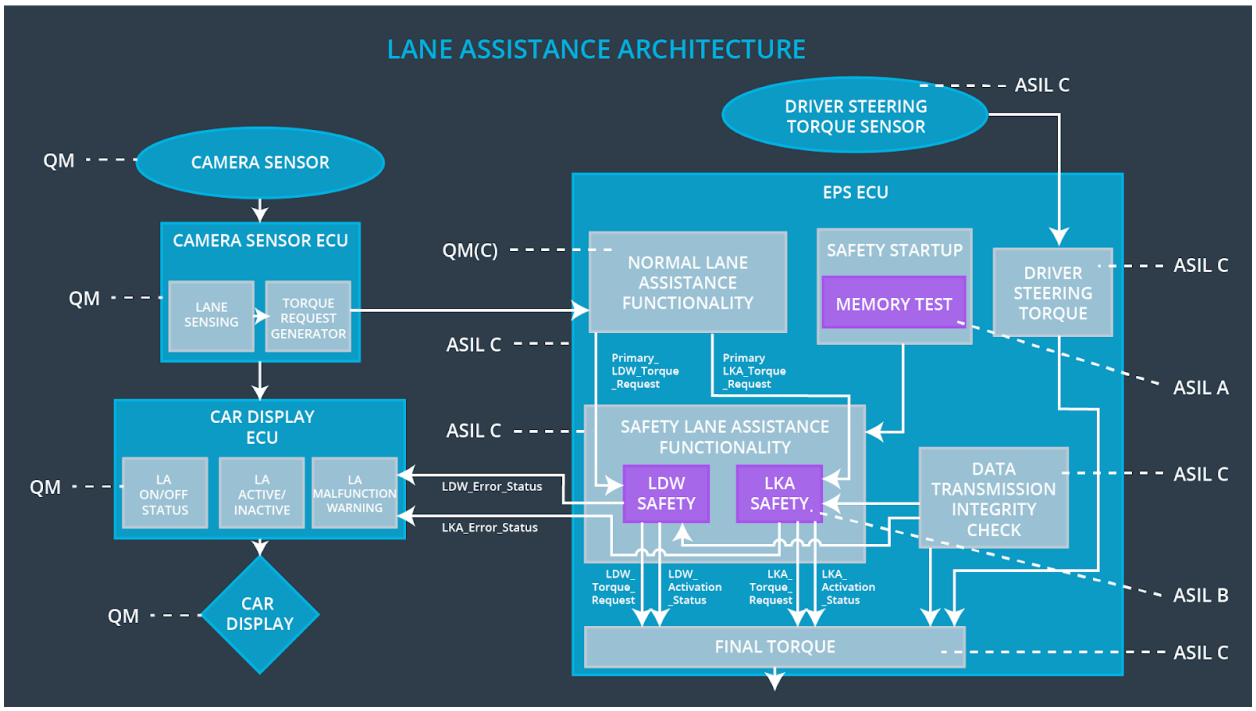
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	‘EPS ECU - LKA Safety’ software block	‘LKA feature’ is deactivated
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	‘EPS ECU - LKA Safety’ software block	‘LKA feature’ is deactivated
Technical Safety Requirement	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and set	B	500 ms	‘EPS ECU - LKA Safety’ software block	‘LKA feature’ is deactivated

03	'LKA_Torque_Request' to 0.				
Technical Safety Requirement 04	The validity and integrity of the data transmission for the signals transmitted shall be ensured.	B	500 ms	‘Data Transmission Integrity Check’	‘LKA feature’ is deactivated
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’	‘LKA feature’ is deactivated

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.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Deactivate the LDW feature	Torque amplitude above Max_Torque_Amplitude, or Torque frequency above	Yes	LDW feature deactivated on the Car Display

		Max_Torque_Frequency		
WDC-02	Deactivate the LKA feature	LKA feature on for more than 500ms time limit	Yes	LKA feature deactivated on the Car Display