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
28th April 2019	1	John Reilly	First Attempt

Table of Contents

Purpose of the Technical Safety Concept

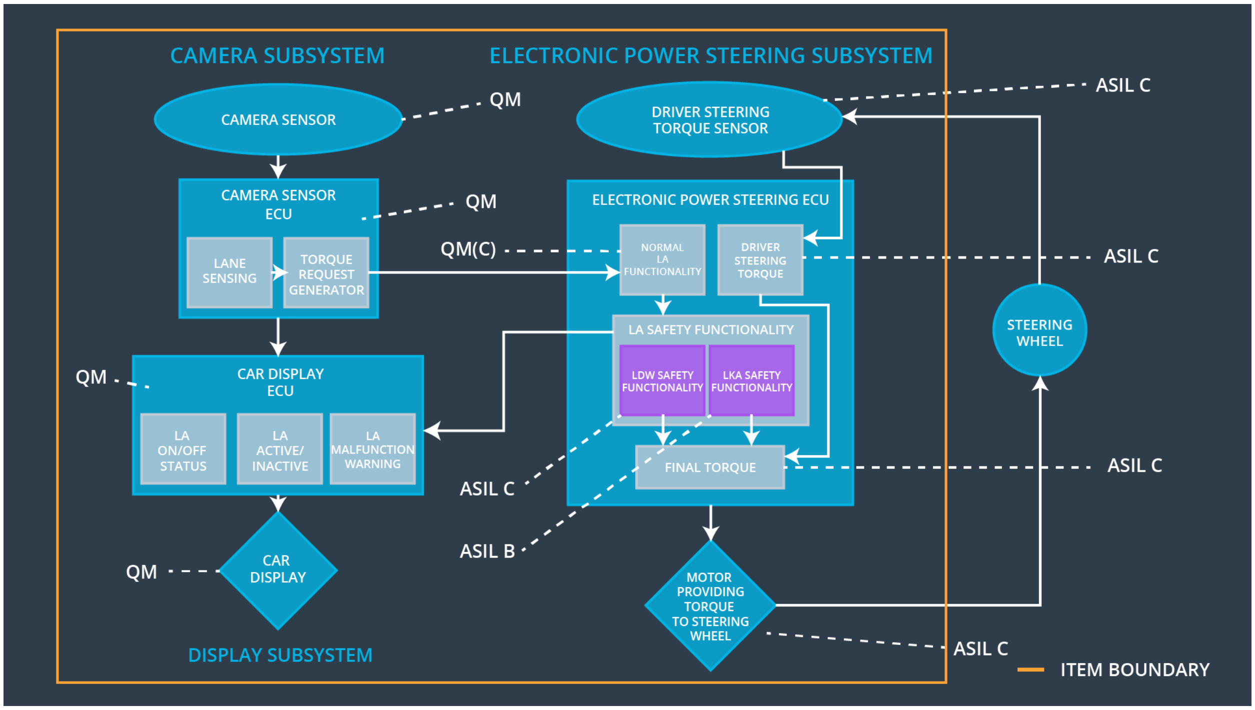
The Technical Safety Concept defines how the subsystems interact at the message level and describes how the ECU's communicate with each other.

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	50ms	Oscillating torque amplitude is below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Oscillating torque 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 for only Max_Duration.	B	500ms	Lane keeping assistance torque is no longer applied.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

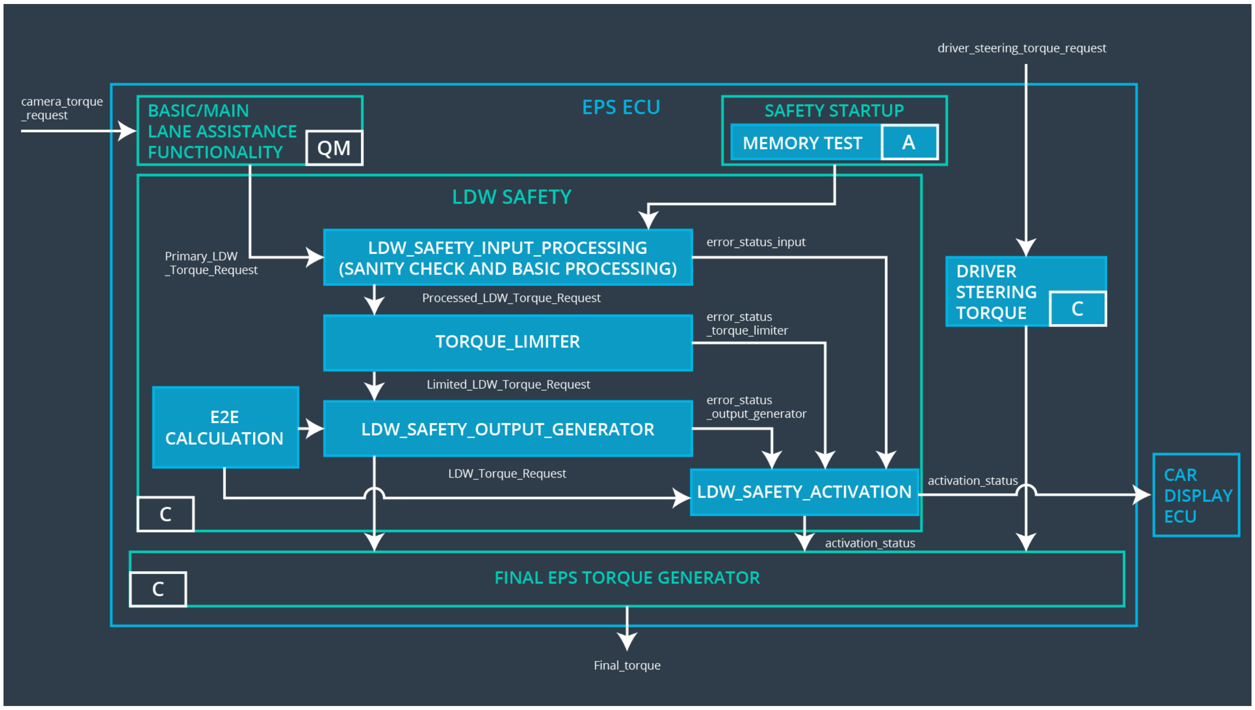
Element	Description
Camera Sensor	Detects optical imformation from the road ahead of the vehicle and send this information to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Software Module , Processes information from the camera sensor to detect lanes ahead of the vehicle
Camera Sensor ECU - Torque request generator	Software Module , Creates a request for a torque to be applied to the steering wheel based on information about lane position
Car Display	Displays messages and information about the car to the driver
Car Display ECU - Lane Assistance On/Off Status	Displays Lane Assistance status with on/off light
Car Display ECU - Lane Assistant	Displays Lane Assistance active or not active

Active/Inactive	indication
Car Display ECU - Lane Assistance malfunction warning	Displays Lane Assistance active or not active indication
Driver Steering Torque Sensor	**Detects the amount of torque currently being applied to the steering wheel**
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Controls the Power Steering subsystem
EPS ECU - Normal Lane Assistance Functionality	Software Module to receive information from Torques request generator under normal functionality
EPS ECU - Lane Departure Warning Safety Functionality	Software Module to ensure Torque frequncy and amplititude are below defined maximum levels
EPS ECU - Lane Keeping Assistant Safety Functionality	Software Module to ensure LKA functionality is not applied longer than defined time duration
EPS ECU - Final Torque	Software Module to combine outputs from EPS ECU Lane Departure Warning Safety Functionality and EPS ECU - Lane Keeping Assistant Safety Functionality and generates an output Torque value.
Motor	Receives control information from the Power Steering ECU and acuates the Steering wheel acordingly

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 Requirem ent 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	50ms	LDW Safety	Torque applied to steering wheel is zero
Technical Safety	As soon as the LDW function deactivates the LDW feature,	C	50ms	LDW Safety	Torque applied to

Requirement 02	the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.				steering wheel is 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	50ms	LDW Safety	Torque applied to steering wheel is zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	LDW Safety	Torque applied to steering wheel is 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 Start-Up	Torque applied to steering wheel 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 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_Frequency.	C	50ms	LDW Safety	Torque applied to steering wheel is 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	50ms	LDW Safety	Torque applied to steering wheel is 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	50ms	LDW Safety	Torque applied to steering wheel is zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	LDW Safety	Torque applied to steering wheel is 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 Start-Up	Torque applied to steering wheel is zero

Lane Keeping Assistance (LKA) Requirements:

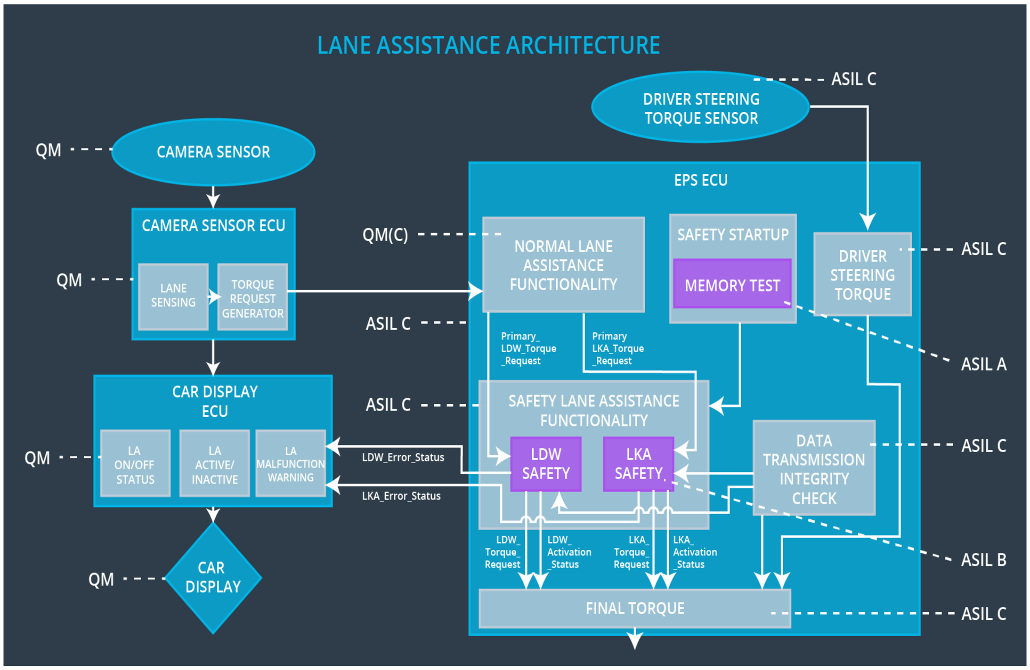
Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

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 that the LKA function is applied for a maximum time duration defined as MAX_DURATION	C	500ms	LDW Safety	Torque applied to steering wheel is 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.	C	500ms	LDW Safety	Torque applied to steering wheel is zero
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	C	500ms	LDW Safety	Torque applied to steering wheel is zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500ms	LDW Safety	Torque applied to steering wheel is 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 Start-Up	Torque applied to steering wheel is 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 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_Frequency.	X		
Technical Safety Requirement 01-01-02	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.	X		

Technical Safety Requirement 01-01-03	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.	X		
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	X		
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	X		
Technical Safety Requirement 01-02-01	The LKA safety component shall ensure that the LKA function is applied for a maximum time duration defined as MAX_DURATION	X		
Technical Safety Requirement 01-02-02	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.	X		
Technical Safety Requirement 01-02-03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	X		
Technical Safety Requirement 01-02-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	X		
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	X		
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure that the LKA function is applied for a maximum time duration defined as MAX_DURATION	X		
Technical Safety Requirement 02-01-02	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display	X		

	ECU to turn on a warning light.			
Technical Safety Requirement 02-01-03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	X		
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	X		
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	X		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn Off Lane Departure Warning Function	Malfunction_01 Malfunction_02	YES	Dashboard Warning Light/ Warning Message on Display
WDC-02	Turn Off Lane Keeping Function	Malfunction_03	YES	Dashboard Warning Light/ Warning Message on Display