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
11/10/2017	1.0	Pedro Lizana	First version of the document.

Table of Contents

Purpose of the Technical Safety Concept

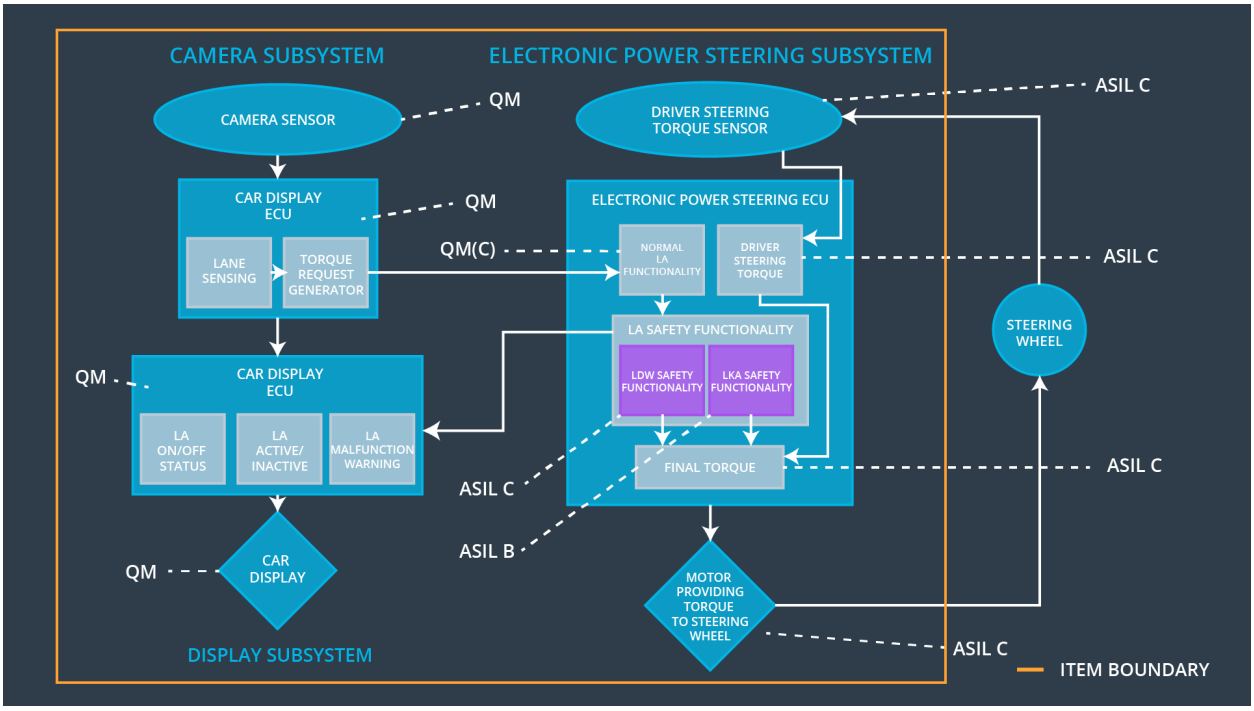
The Technical Safety Concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	The Safe State is achieved when the LDW function is turned off (Lane Assistance Output = 0).
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency.	C	50ms	The Safe State is achieved when the LDW function is turned off (Lane Assistance Output = 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	500ms	The Safe State is achieved when the LKA function is turned off (Lane Assistance Output = 0).

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 has accidentally departed its ego lane and sends this output to the Camera Sensor ECU - Torque request generator.
Camera Sensor ECU - Torque request generator	The Camera Sensor ECU – Torque Request Generator uses the output of the The Camera Sensor ECU – Lane Sensing functionality to calculate the torque to keep the vehicle in the same lane and the torque to warn the driver that is has departed its ego lane. It then sends this messages (torque requests) to the Car Display ECU and to Normal Lane Assistance functionality in the Electronic Power Steering ECU.

Car Display	The Car Display shows information related to the Lane Assistance item and other items as well.
Car Display ECU - Lane Assistance On/Off Status	Controls the light that tells the driver if the Lane Assistance feature is On or Off.
Car Display ECU - Lane Assistant Active/Inactive	Controls the light that tells the driver if the Lane Assistance feature is Active or Inactive.
Car Display ECU - Lane Assistance malfunction warning	Controls the light that tells the driver if there is a malfunction with the Lane Assistance feature.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor measures the current torque in the steering wheel, information passed to the Driver Steering Torque functionality in the Electronic Power Steering ECU.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives the information from the Driver Steering Torque Sensor and sends it to the Final Torque Generator functionality.
EPS ECU - Normal Lane Assistance Functionality	Will receive the raw torque request by the Camera Sensor ECU - Torque request generator functionality and limit the torque frequency and amplitude. It send the torque output to the EPS ECU LA Safety Functionalities.
EPS ECU - Lane Departure Warning Safety Functionality	Will check that the torque request from the EPS ECU - Normal Lane Assistance Functionality is below the Max_Torque_Amplitude and Max_Torque_Frequency. If it is higher, then it transmits a error status to the Car Display. If it is lower, then
EPS ECU - Lane Keeping Assistant Safety Functionality	Will check that the LKA normal functionality has not sent LKA torque requests for more than Max_Duration.
EPS ECU - Final Torque	It outputs the final torque to send to the motor. It receives as an input the torque from the Driver Steering Torque and the torque requests from the Safety Lane Assistance Functionality.
Motor	The Motor applies the torque request generated by the EPS ECU – Final Torque functionality.

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	50ms	LDW Safety Block	Lane Departure Warning Torque Request Amplitude Shall be 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	C	50ms	LDW Safety Block	Lane Departure Warning Torque Request

	warning light.				Amplitude Shall be 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	50ms	LDW Safety Block	Lane Departure Warning Torque Request Amplitude 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	50ms	Data Transmission Integrity Check Block	Lane Departure Warning Torque Request Amplitude Shall be 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 Block	Lane Departure Warning Torque Request Amplitude Shall be 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	50ms	LDW Safety Block	Lane Departure Warning Torque Request Frequency Shall be set to zero.
Technical Safety Requirement 02	As soon as the safety 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 Block	Lane Departure Warning Torque Request Frequency Shall be set to zero.
Technical Safety Requirement 03	As soon as a failure is detected by the safety LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	50ms	LDW Safety Block	Lane Departure Warning Torque Request Frequency 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	50ms	Data Transmission Integrity Check Block	Lane Departure Warning Torque Request Frequency Shall be 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 Block	Lane Departure Warning Torque Request Frequency Shall be set to zero.

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

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		

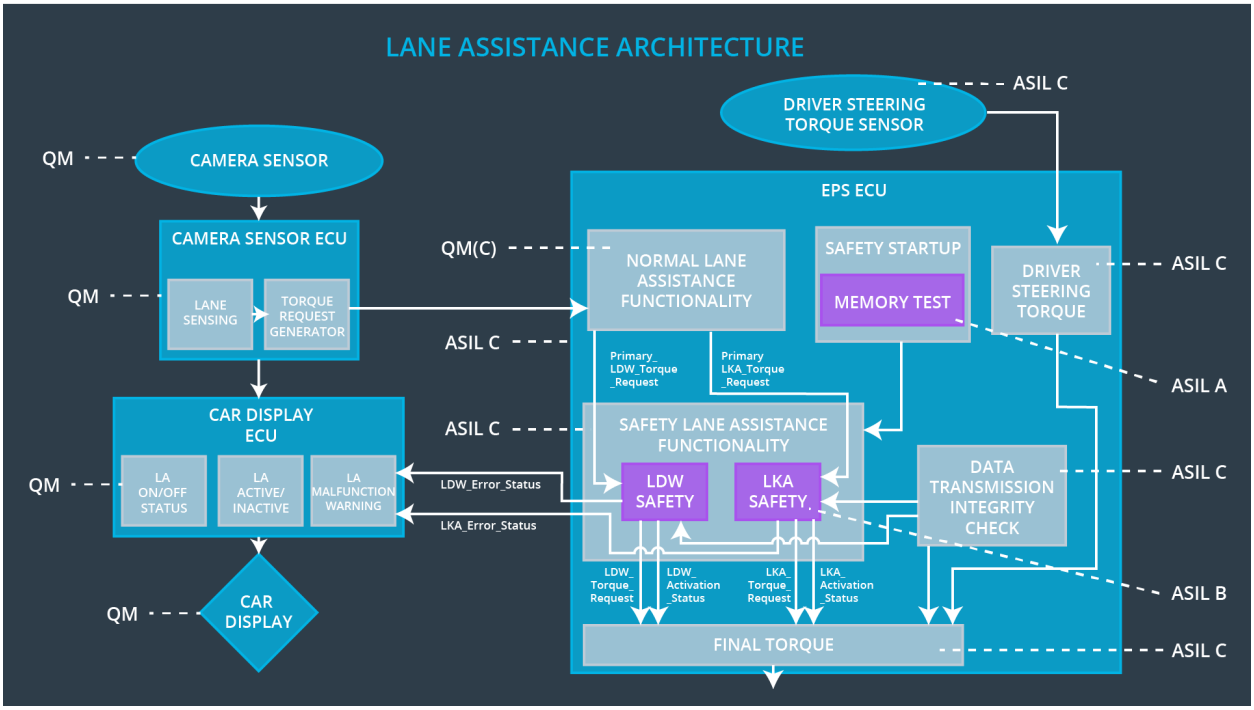
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

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_Torque_Request' sent to the 'Final electronic power steering Torque' component is applied for only ‘Max_Duration’.	B	500ms	LKA Safety Block	Lane Keeping Assistance Torque Request Shall be set to zero.
Technical Safety Requirement 02	As soon as the safety 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	500ms	LKA Safety Block	Lane Keeping Assistance Torque Request Shall be set to zero.
Technical Safety Requirement 03	As soon as a failure is detected by the safety LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	B	500ms	LKA Safety Block	Lane Keeping Assistance Torque Request Shall be set to zero.
Technical Safety Requirem	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal	B	500ms	Data Transmission Integrity	Lane Keeping Assistance Torque Request

ent 04	shall be ensured.			Check Block	Shall be 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 Block	Lane Keeping Assistance Torque Request Shall be set to zero.

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

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

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

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW (LA) functionality.	Torque amplitude and frequency exceeds Max_Torque_Ampltiude or Max_Torque_Frequency.	Yes.	Lane Assistance lights in Car Display will turn to Off/Inactive. The LA Malfunction Warning light will also turn on.
WDC-02	Turn off LKA (LA) functionality.	Duration of LKA exceeds Max_Duration.	Yes.	Lane Assistance lights in Car Display will turn to Off/Inactive. The LA Malfunction Warning light will also turn on.