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
22-05-18	1.0	Akshatha Holla	Technical Safety Concept

Table of Contents

Purpose of the Technical Safety Concept

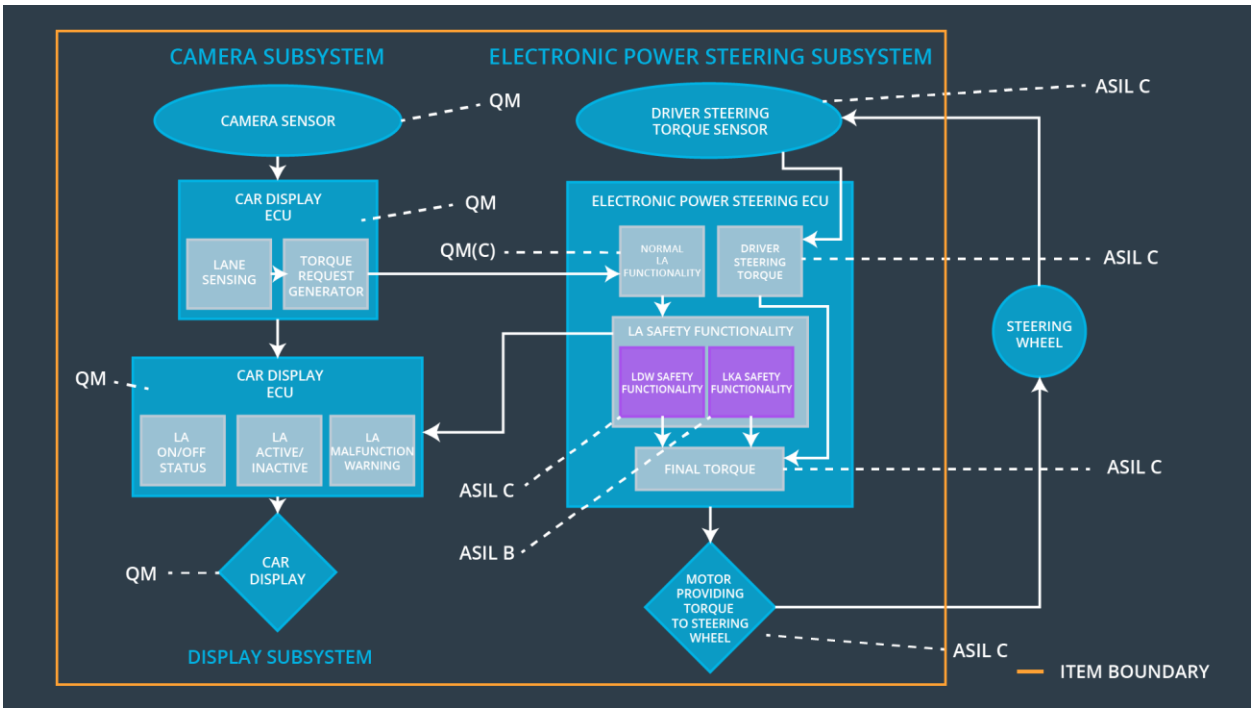
The purpose of the technical safety concept is to convert functional requirements into technical requirements and is more concrete since it gets into the details of the item's technology. As opposed to the functional safety concept which was a part of the concept phase the technical safety concept is a part of the Product development phase.

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	Ensuring that the 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	Ensuring that the torque frequency is below Max_Torque_Frequency
Functional Safety Requirement 02-01	The Lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving	B	500ms	Turn off the Lane keeping assistance function

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	The camera sensor is used to capture images of the road and provides them as an input to the Camera sensor ECU.
Camera Sensor ECU - Lane Sensing	The Camera sensor ECU takes the input from the camera sensor and calculates the position of the car with respect to the lane lines that are detected by it.
Camera Sensor ECU - Torque request generator	The Camera sensor ECU –torque generator calculates the torque required to re-center the vehicle according to the lane
Car Display	Provides visual warnings in cases of lane departure and other issues.
Car Display ECU - Lane Assistance On/Off Status	The information about the On/Off status of the Lane Assistance system is

	provided to the car display by the Car Display ECU - Lane Assistance On/Off Status
Car Display ECU - Lane Assistant Active/Inactive	The information about the active/inactive status of the Lane assistance system is provided to the car display by the Car Display ECU - Lane Assistant Active/Inactive
Car Display ECU - Lane Assistance malfunction warning	The information about possible malfunctions in the Lane assistance system is provided to the car display by the Car Display ECU - Lane Assistance malfunction warning
Driver Steering Torque Sensor	Driver Steering Torque Sensor measures the amount of torque applied by the driver to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes the driver steering torque measured by the driver steering torque sensor.
EPS ECU - Normal Lane Assistance Functionality	Performs Lane assistance functions like Lane departure warning and Lane keeping assistance. Takes necessary torque inputs from camera sensor ECU and generates necessary final torque.
EPS ECU - Lane Departure Warning Safety Functionality	Ensures that the applied torque amplitude and frequency are minimum.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures that the Lane Keeping assistance function is not activated longer than Max_Duration.
EPS ECU - Final Torque	Combine the outputs of Lane Departure Warning Safety Functionality, Lane Keeping Assistant Safety Functionality and Electronic Power Steering (EPS) ECU - Driver Steering Torque to calculate final torque
Motor	Takes appropriate torque input from Electronic Power steering ECU and applies it 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	50ms	LDW_safety	LDW_Torque _Request is set to zero
Technical Safety Requirement 02	As soon as the failure is detected by the LDW function, it shall de activate the LDW feature and the LDW_torque_Request shall be set to zero.	C	50ms	LDW_safety	LDW_Torque _Request is set to zero

Technical Safety Requirement 03	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	LDW_Torque_Request is set to zero
Technical Safety Requirement 04	Memory test shall be conducted at the start up of the EPS ECU to check for any faults in memory	A	Ignition cycle	Safety start up	LDW_Torque_Request is set to zero
Technical Safety Requirement 05	The validity and Integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50ms	Data Transmission Integrity check	LDW_Torque_Request 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	50ms	LDW_safety	LDW_Torque_Request is set to zero
Technical Safety Requirement 02	As soon as the failure is detected by the LDW function, it shall de activate the LDW feature and the LDW_torque_Request shall be set to zero.	C	50ms	LDW_safety	LDW_Torque_Request is set to zero
Technical Safety Requirement 03	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	LDW_Torque_Request is set to zero
Technical Safety Requirement 04	Memory test shall be conducted at the start up of the EPS ECU to check for any faults in memory	A	Ignition cycle	Safety start up	LDW_Torque_Request is set to zero
Technical Safety Requirement 05	The validity and Integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50ms	Data Transmission Integrity check	LDW_Torque_Request 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)

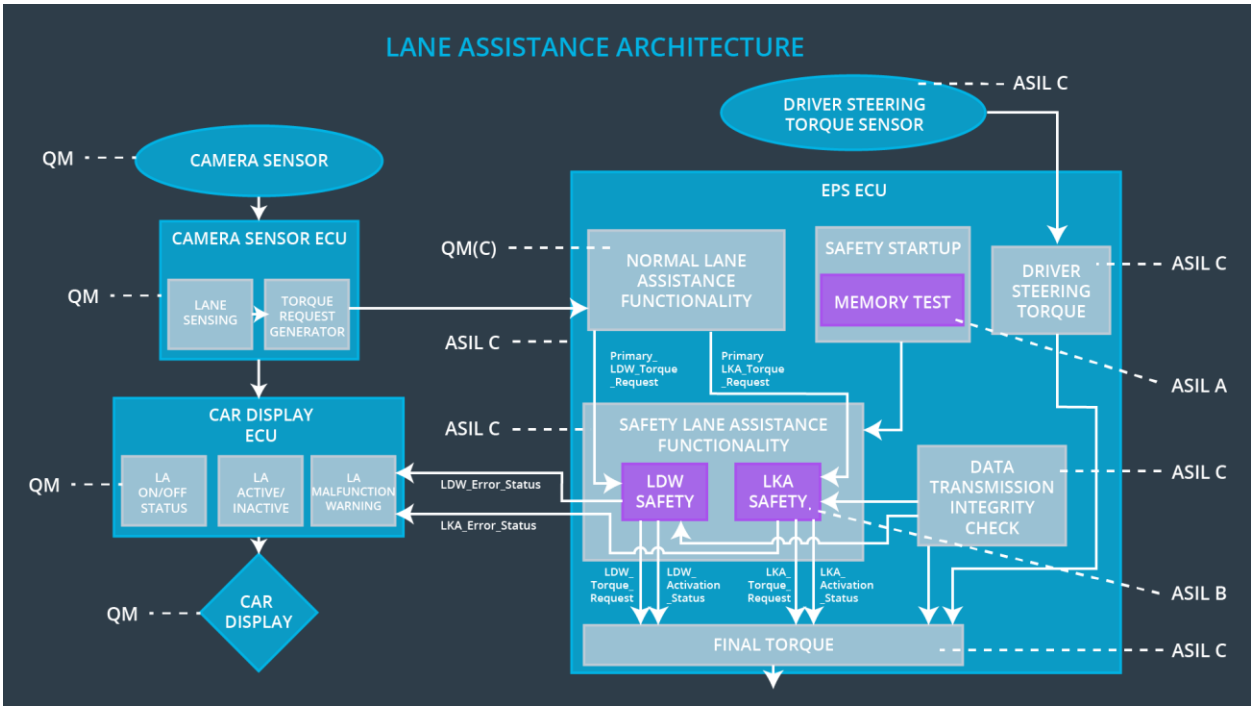
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 that the duration of the LKA_Torque_Request sent to the Final Electronic Power Steering Torque component is below Max_Duration	B	500ms	LKA_safety	LKA_Torque_Request is set to zero
Technical Safety Requirement 02	Memory test shall be conducted at the start up of the EPS ECU to check for any faults in memory	A	Ignition cycle	Safety start up	LKA_Torque_Request is set to zero
Technical Safety Requirement 03	The validity and Integrity of the data transmission for LKA_Torque_Request signal shall be ensured	B	500ms	Data Transmission Integrity check	LKA_Torque_Request is set to zero
Technical Safety Requirement 04	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	500ms	LKA_safety	LKA_Torque_Request is set to zero

Technical Safety Requirement 05	As soon as the failure is detected by the LKA function, it shall de activate the LKA feature and the LKA_torque_Request shall be set to zero.	B	500ms	LKA_safety	LKA_Torque_Request is set to zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

Here you can state that for this particular item, 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	Turn off LDW functionality	Malfunction_01 Malfunction_02	Yes	Lane departure Warning on car display
WDC-02	Turn off LKA functionality	Malfunction_03	Yes	LKA Warning on display