Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
5/24/2018	1.0	Ninad K	Initial Draft
5/25/2018	1.1	Ninad K	Made changes to Safety Concept information as per reviewer's comments

Table of Contents

Purpose of the Technical Safety Concept

The goal of the Technical Safety Concept is to use the functional safety requirements to define technical safety requirements and do allocate the technical safety requirements to the system architecture.

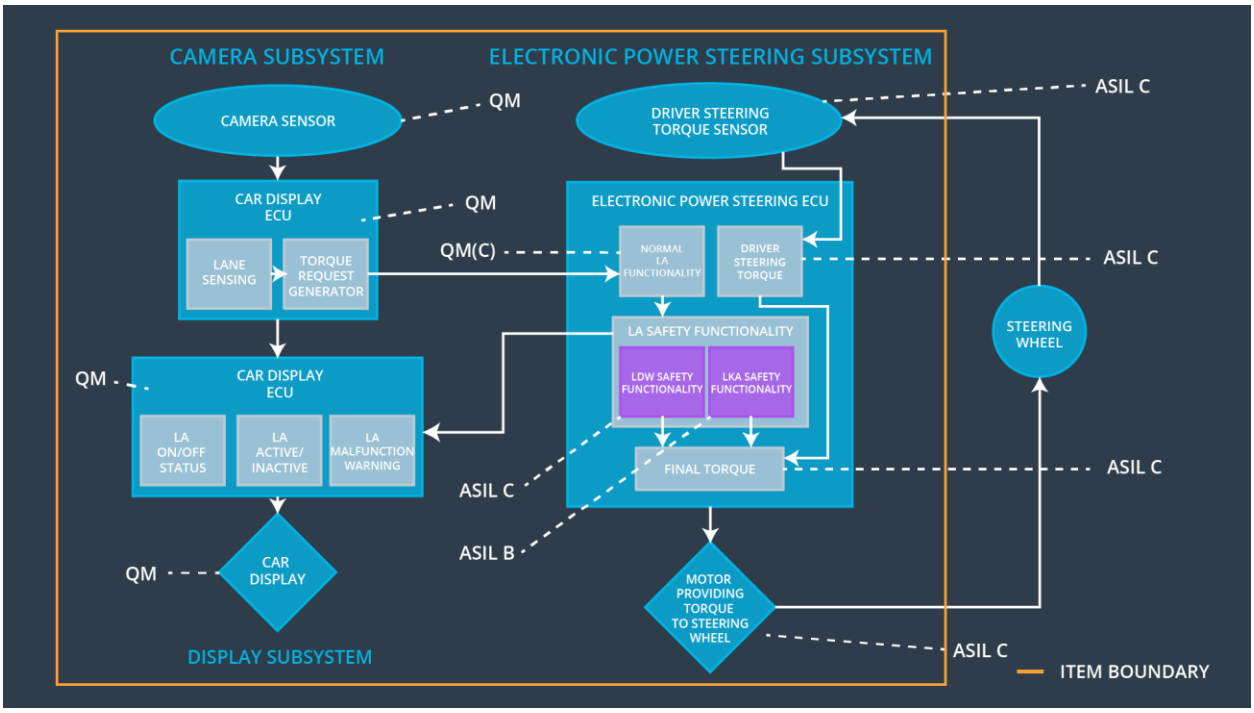
The technical safety requirements are needed for the development of the hardware and software components.

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.	The vibrational oscillating torque's 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	50 ms.	The vibrational oscillating torque's 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	500 ms.	The torque applied by the power steering ECU after Max_Duration is 0.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	This is the vision input source and the images from this sensor are forwarded to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Utilizes the camera images to detect lane lines and determine if the vehicle is in the correct position.
Camera Sensor ECU - Torque request generator	Based on the lane position, determines how much torque is required to steer in the correct direction and then sends a torque request to the EPS ECU.
Car Display	Displays warnings to the driver based on information received from the Car Display ECU.
Car Display ECU - Lane Assistance On/Off Status	Notifies the driver whether the Lane Assistance System is enabled via a light on the dashboard.

Car Display ECU - Lane Assistant Active/Inactive	Notifies the driver whether the Lane Assistance System is currently active and attempting to steer the vehicle.
Car Display ECU - Lane Assistance malfunction warning	Notifies the driver whether the Lane Assistance System has malfunctioned through a light on the dashboard.
Driver Steering Torque Sensor	Detects the current steering torque and forwards the same to the EPS ECU.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	This component processes the torque applied by the driver on the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Receives the input from the Camera Sensor ECU and forwards it to the LA Safety Functionality subsystem.
EPS ECU - Lane Departure Warning Safety Functionality	Makes sure that the LDW steering torque meets the functional safety requirements in terms of amplitude and frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Makes sure that the LKA steering torque meets the functional safety requirements in terms of active duration.
EPS ECU - Final Torque	Processes the safe steering torque requested by the LA Safety component and forwards it to the Motor.
Motor	Based on the data sent by the EPS ECU, a torque is applied to the steering.

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_Request Amplitude is 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	LDW Safety	LDW_Torque_Request Amplitude is 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	LDW Safety	LDW function is stopped.
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 Amplitude is 0.
Technical Safety Requirem	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Memory Test	LDW_Torque_Request Amplitude is

ent 05					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	LDW Safety	LDW_Torque_Request Frequency is 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	LDW Safety	LDW_Torque_Request Frequency is 0.
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 function is

03	'**LDW_Torque_Request**' shall be set to zero.				stopped.
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 Frequency is 0.
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	Memory Test	LDW_Torque_Request Frequency is 0.

Lane Keeping Assistance (LKA) Requirements:

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

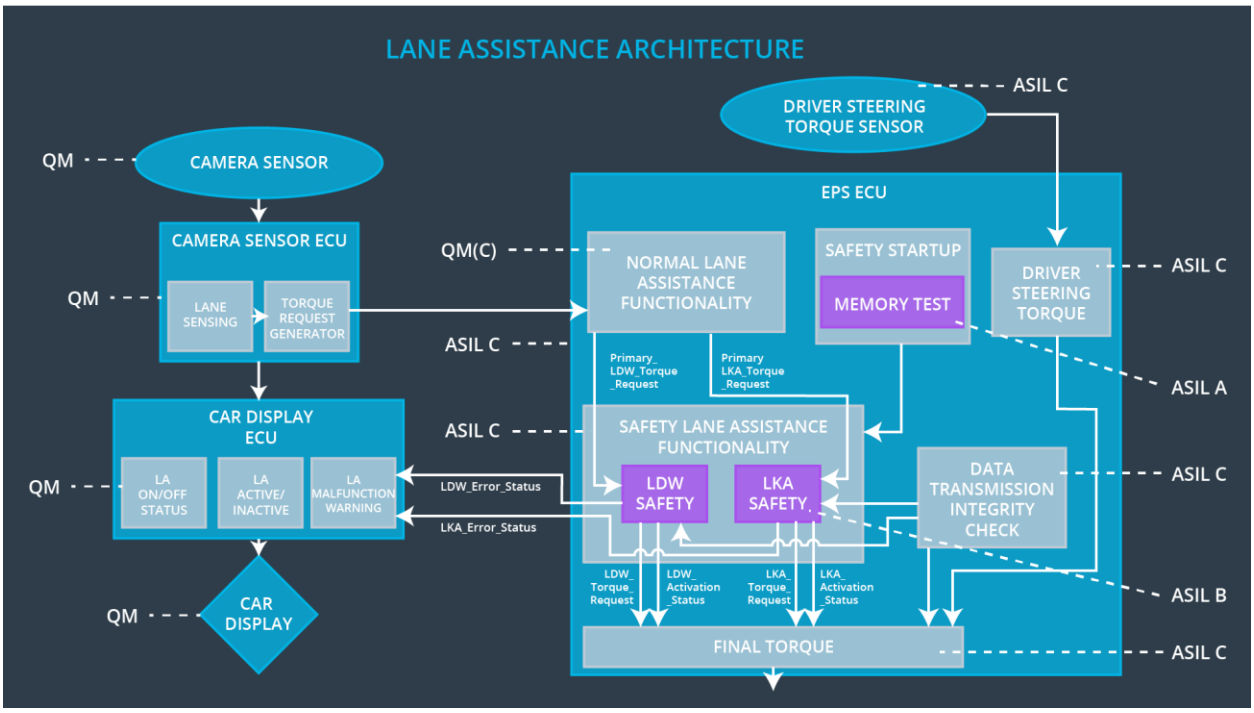
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only **Max_Duration**	X		

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 function shall ensure that the '**LKA_Torque_Request'** is sent for a duration not longer than **Max_Duration.**	B	500 ms	LKA Safety	LKA Torque Request is 0.

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	LKA Torque Request is 0.
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.	B	500 ms	LKA Safety	LKA function is turned off.
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 Request is 0.
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	Memory Test	LKA Torque Request is 0.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All the technical safety requirements are allocated to the EPS ECU. The **Technical Safety Requirements** table located above in this document specifies the exact component to which each requirement is allocated.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane Assistance System is turned off.	Malfunction_01 OR Malfunction_02	Yes	Warning displayed on the Car Display.
WDC-02	Lane Assistance System is turned off.	Malfunction_03	Yes	Warning displayed on the Car Display.