Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: Version 1.1, Released on 2018-11-21

Document history

Date	Version	Editor	Description
11/18/18	1.0	Emile Papillon	First Draft
11/21/18	1.1	Emile Papillon	Revision and Release

Table of Contents

Purpose of the Technical Safety Concept

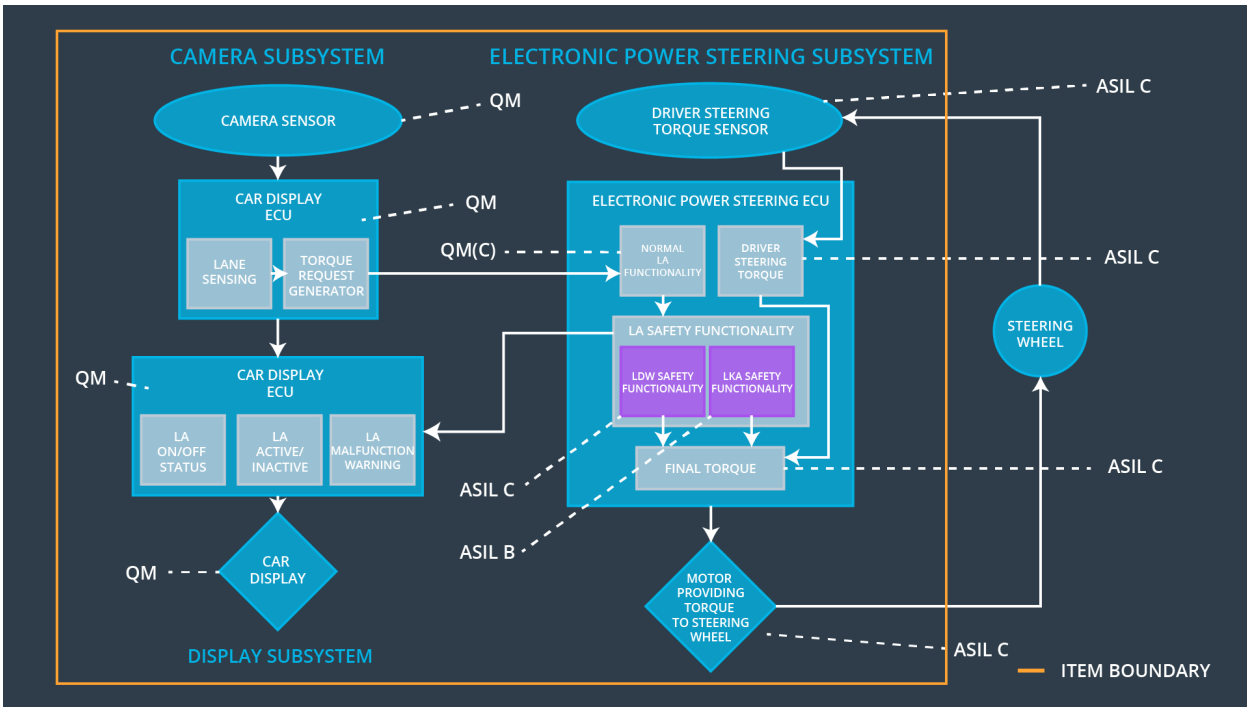
The technical safety concept derives more specific, technically focued requirements from the functional safety requirement. These requirements are then allocated to elements of the architecture in a process similar to what was done previously in the functional safety concept.

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 chosen amplitude threshold Max_Torque_Amplitude is low enough to make the system safe.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The chosen frequency Max_Torque_Frequency is low enough to make the system safe	C	50 ms	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement 02-01	The Lane Keeping Assistance shall be limited in time to a duration of Lane_Keeping_Timeout after which the feature turns off	B	500 ms	Lane Keeping turns off after Lane_Keeping_Timeout

Refined System Architecture from Functional Safety Concept

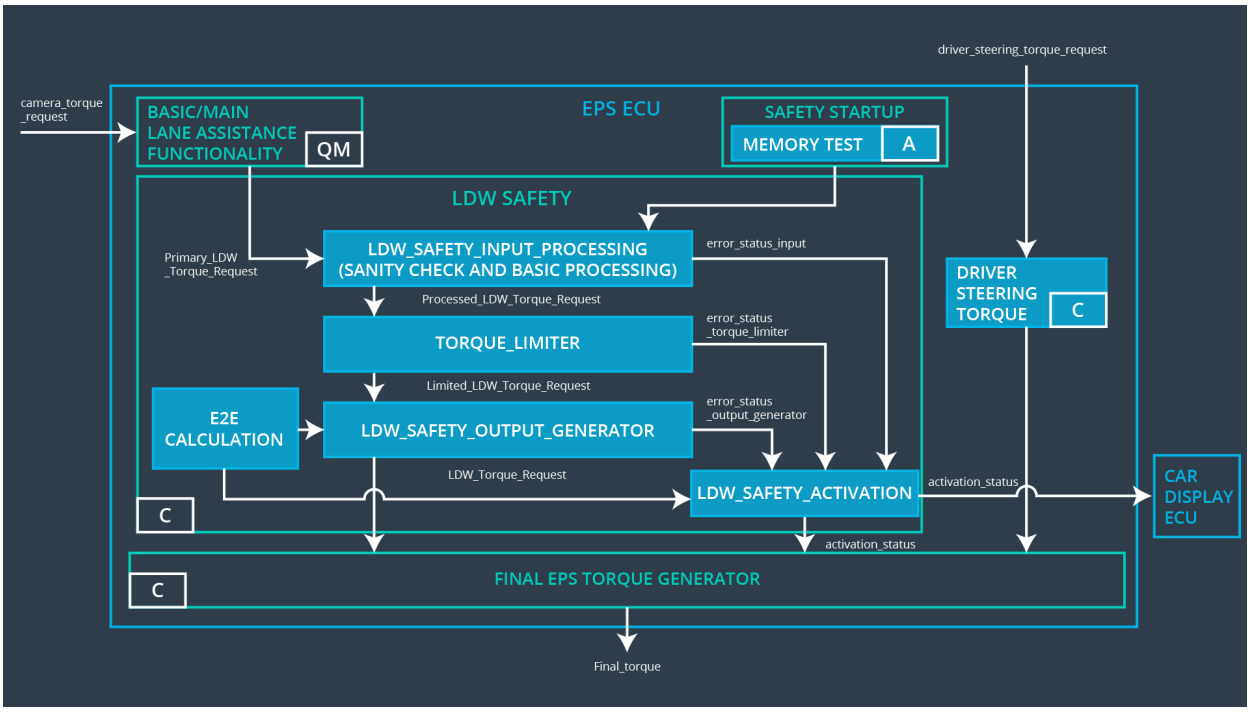


Functional overview of architecture elements

Element	Description
Camera Sensor	Responsible for detecting the lines
Camera Sensor ECU - Lane Sensing	Responsible of processing the data captured by the camera sensor and determining when the vehicle leaves the lane by mistake
Camera Sensor ECU - Torque request generator	Responsible of calculating the torque requested by the system to the motor
Car Display	Interface with the human driver displaying system status and fault/malfunction warnings
Car Display ECU - Lane Assistance On/Off Status	Display the status of the Lane Assistance (On/Off) via the Car Display (HMI)
Car Display ECU - Lane Assistant Active/Inactive	Display the status of the Lane Assistance (Active/Inactive).

Car Display ECU - Lane Assistance malfunction warning	Displays Lane Assistance malfunctions through the Car Display (HMI)
Driver Steering Torque Sensor	Senses the torque input by the driver to provide just the right amount of extra torque for lane keeping assistance
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Deterimines the torque applied by the driver to calculate the torque request
EPS ECU - Normal Lane Assistance Functionality	Relays the torque request from the Camera ECU to the motor during normal operation.
EPS ECU - Lane Departure Warning Safety Functionality	Ensures the amplitude of the requested torque is below Max_Torque_A mplitude and the frequency below Max_Torque_Fr equency..
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures the LKA is not active for more than the specified Lane_Keeping_Timeout
EPS ECU - Final Torque	Ensures the torque is within allowed boundaries
Motor	Applies torque to the steering wheel/column.

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 is set to zero.
Technical Safety Requirement 02	When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	LDW torque is set to zero.
Technical Safety Requirement 03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set ‘LDW_Torque_Request’ to zero.	C	50 ms	LDW Safety	LDW torque is set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	LDW Safety	LDW torque is 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	Data Transmissio n Integrity Check	LDW torque 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 amplitude 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 is set to zero.

* This requirement also bears the requirements listed for FSR 01-01.

Lane Keeping Assistance (LKA) Requirements:

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

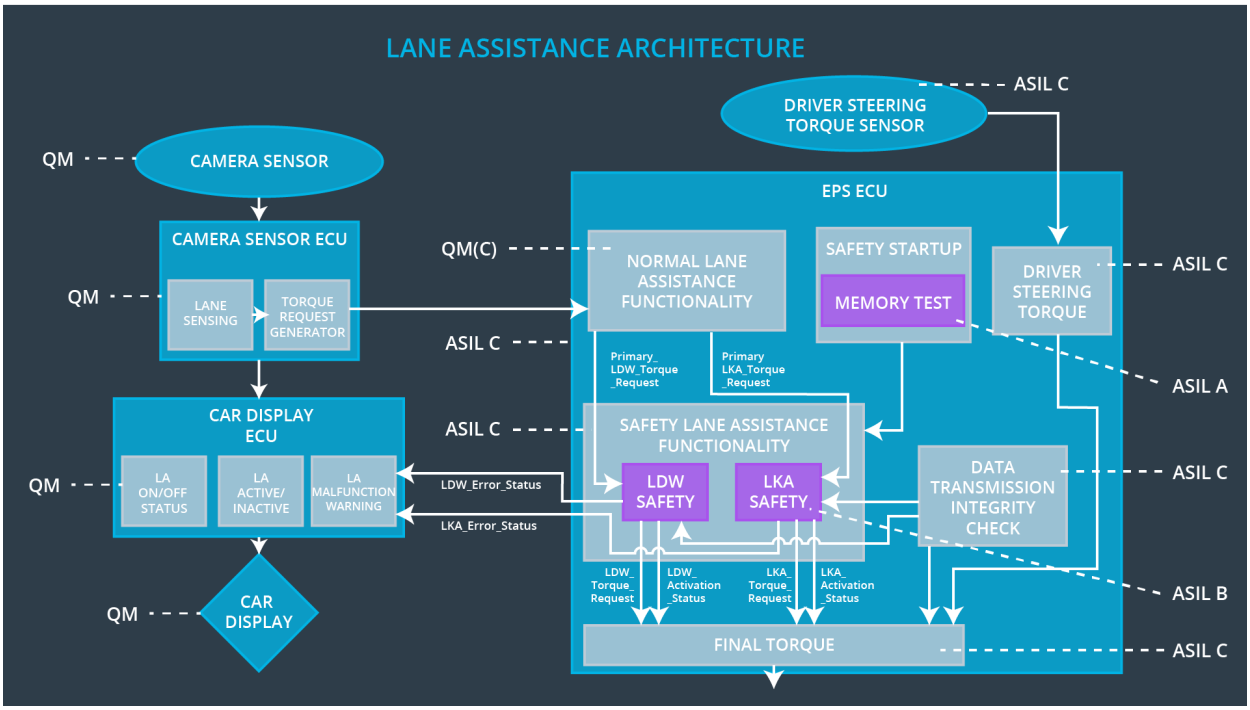
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Lane_Keeping_Timeout	C	500 ms	LKA Safety	LKA torque is set to zero
Technical Safety Requirement 02	When the Lane Keeping Assist is deactivated, the ‘LKA Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	500 ms	LKA Safety	LKA torque is set to zero.
Technical Safety Requirement 03	When a failure is detected by the Lane Keeping Assist functionality, it shall deactivate the Lane Keeping Assist feature and set ‘LKA_Torque_Request’ to zero.	C	500 ms	LKA Safety	LKA torque is set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500 ms	LKA Safety	LKA torque is 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	Data Transmissio n Integrity Check	LKA torque is set to zero.

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	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02, Malfunction_05	Yes	LDW malfunction Warning light on Car Display

	completely			
WDC-02	Turn off Lane Keeping Assistance functionality completely	Malfunction_03, Malfunction_04, Malfunction_05	Yes	LKA malfunction Warning light on Car Display