Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
12/3/17	1.0	Vatche Donikian	First submission attempt

Table of Contents

Purpose of the Technical Safety Concept

The technical safety concept is used to turn functional safety requirements into technical safety requirements, essentially allocating those requirements to the system architecture and involving hardware and software.

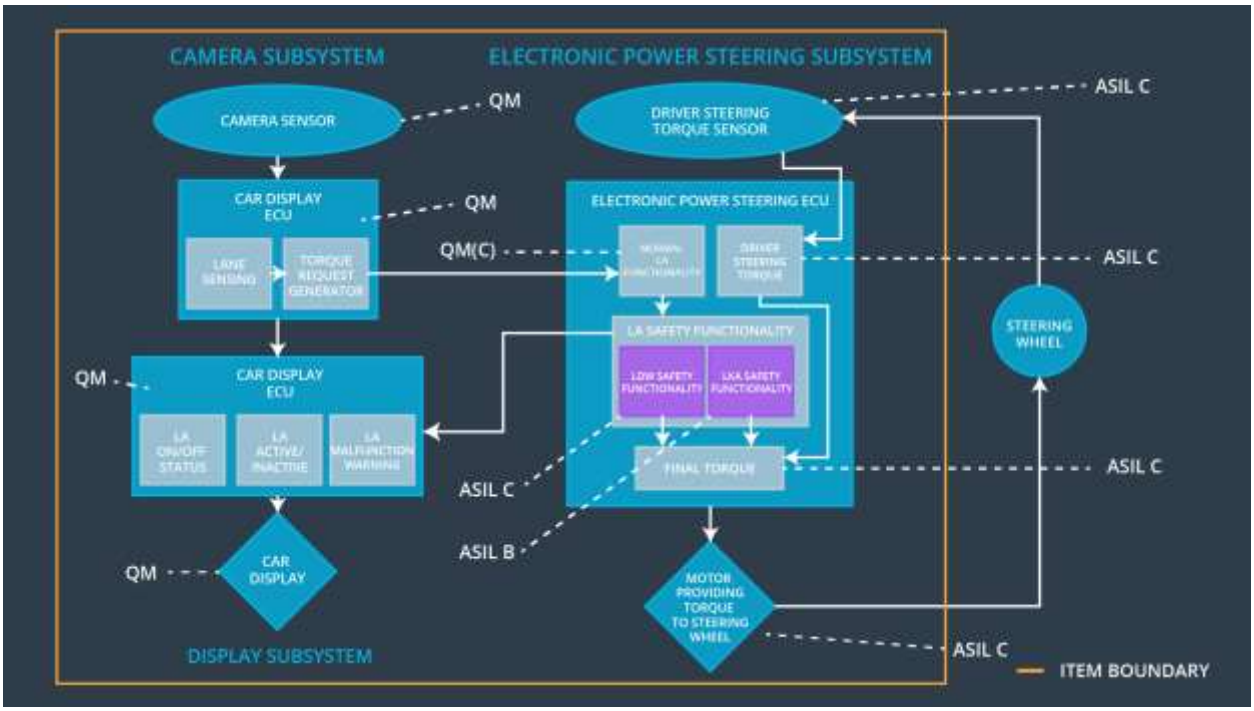
Inputs to the Technical Safety Concept

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	Turn function off
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	Turn function off
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	Turn function off

Refined System Architecture from Functional Safety Concept

The refined system architecture is shown below, with each component of the item allocated with an ASIL score.



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures images of the road
Camera Sensor ECU - Lane Sensing	Determines when the vehicle is leaving the lane
Camera Sensor ECU - Torque request generator	Requests an EPS torque to correct for lane drift or an oscillating torque for driver alerting
Car Display	Lights up to notify driver of lane departure
Car Display ECU - Lane Assistance On/Off Status	Determines when to light up the dash to notify driver of lane assistance status
Car Display ECU - Lane Assistant Active/Inactive	Determines when to light up dash to notify driver of lane assistance being active or not
Car Display ECU - Lane Assistance malfunction warning	Determines when to light up dash to notify driver of a malfunction in the lane assistance item
Driver Steering Torque Sensor	Determines the amount, if any, that the driver is steering

Electronic Power Steering (EPS) ECU - Driver Steering Torque	Determines if the driver is responding to the lane departure warning or if the hands are completely off the wheel
EPS ECU - Normal Lane Assistance Functionality	Determines the amount of torque request to send to the motor, if determined by camera system
EPS ECU - Lane Departure Warning Safety Functionality	Sends an oscillating torque command to the motor at specified frequency and amplitude and sends signal to car display ECU
EPS ECU - Lane Keeping Assistant Safety Functionality	Sends an assitive torque command to the motor at specified amount and duration and sends signal to car display ECU
EPS ECU - Final Torque	Final torque sent to the motor
Motor	Applies torque 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	50 ms	LDW Safety software component of EPS ECU	The LDW 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 warning light.	C	50 ms	LDW Safety software component of EPS ECU	The LDW torque request 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	50 ms	LDW Safety software component of EPS ECU	The LDW 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	50 ms	Data transmission integrity check	The LDW torque request amplitude shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup Memory Test block	The LDW 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 amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Frequency.	C	50 ms	LDW Safety software component of EPS ECU	The LDW torque request frequency 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 warning light.	C	50 ms	LDW Safety software component of EPS ECU	The LDW torque request frequency 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	50 ms	LDW Safety software component of EPS ECU	The LDW 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	50 ms	Data transmission integrity check	The LDW torque request frequency shall be set to zero.
Technical Safety	Memory test shall be conducted	A	Ignition cycle	Safety Startup Memory Test	The LDW torque

Requirement 05	at startup of the EPS ECU to check for any faults in memory.			block	request frequency shall be 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		

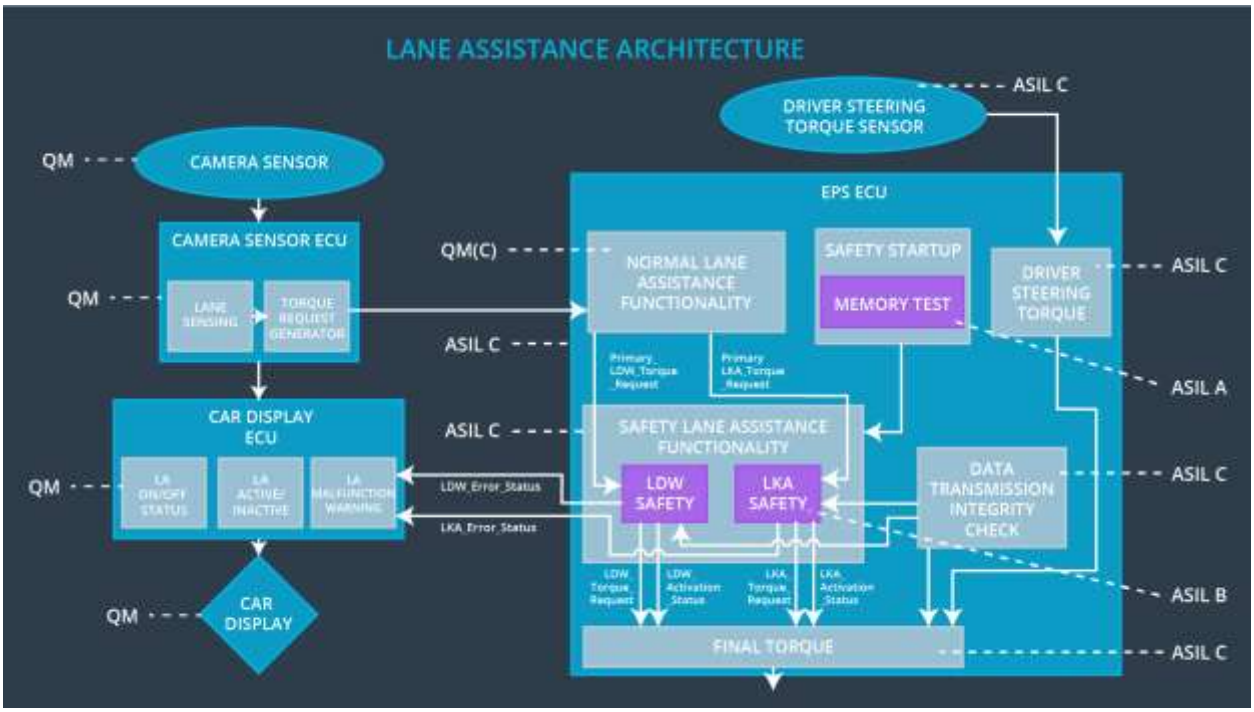
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The Lane Keep Assist 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	500 ms	LKA Safety software component of EPS ECU	The LKA torque request shall be set to 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.	B	500 ms	LKA Safety software component of EPS ECU	The LKA torque request shall be set to 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.	B	500 ms	LKA Safety software component of EPS ECU	The LKA torque request shall be set to zero.

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	The LKA torque request shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup Memory Test block	The LKA torque request shall be set to zero.

Refinement of the System Architecture

The refined system architecture is shown below. It consists of modified ECU blocks which specify what signals are sent, safety checks, and ASIL scores for each individual component.



Allocation of Technical Safety Requirements to Architecture Elements

For the lane assistance 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 functionality	Malfunction_01 & Malfunction_02	Yes	Warning light on the dash
WDC-02	Turn off functionality	Malfunction_03	Yes	Warning light on the dash